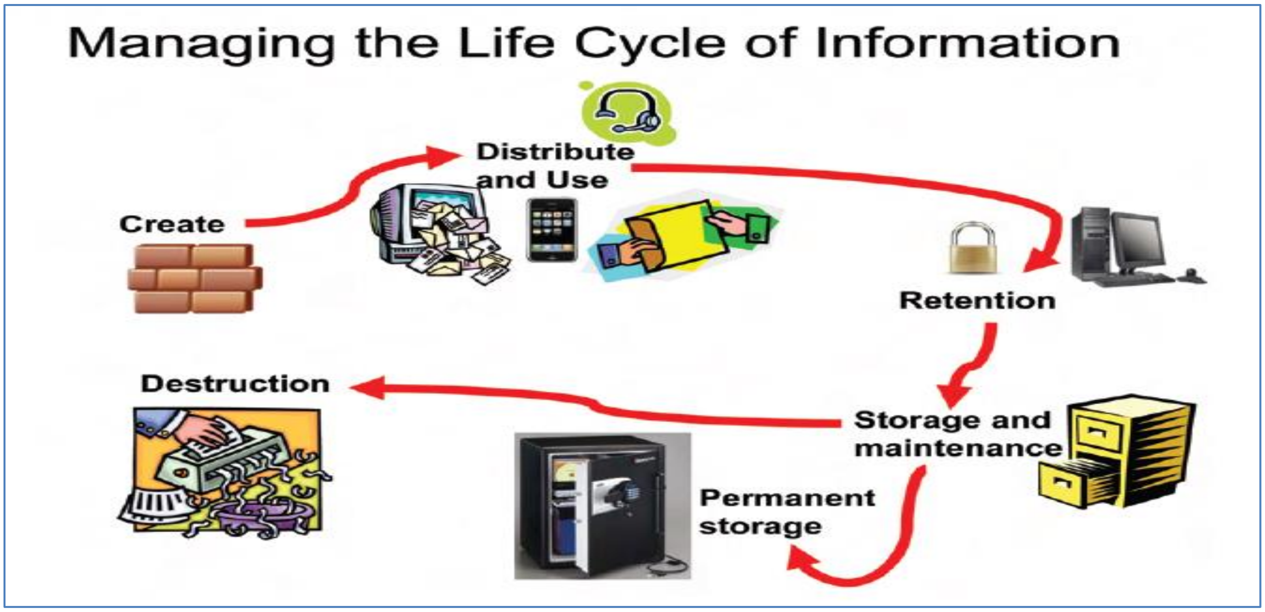
NOT ANONYMOUS ANYMORE: MANAGING PRIVACY CONCERNS

Matt Dugas, Associate, McCague Borlack LLP

The intersection between cyber-risk and privacy: Best practices and takeaways

A new risk has entered the marketplace. It is called cyber-risk, and it is responsible for the equivalent of millions of dollars in lost revenue, client loyalty, and goodwill. For the purposes of this paper, cyber risk relates to the mishandling of customer information (CI) throughout its acquisition, retention and destruction – what some business analysts refer to as the lifecycle of customer data. The privacy of CI has become paramount as companies continue to struggle with data management and the ensuing loss of consumer confidence.

As a corporate concept, risk is not new. Insurance companies are in the business of risk. It is what they do, and they manage it well. This paper discusses the management of cyber risk and, specifically, how to implement and execute an effective privacy management program (PMP).



The lifecycle of personal information[19]

[19] Privacy Risk Management: Building privacy protection into a Risk Management Framework to ensure that privacy risks are managed, by default . Online: Information and Privacy Commissioner of Ontario <http://www.ipc.on.ca/images/Resources/pbd-priv-risk-mgmt.pdf>.

A SHIFT IN PERSPECTIVE

As privacy concerns have become more prevalent, so has the public's sensitivity to privacy breaches. The protection of customer information is no longer an afterthought. People expect and demand that their personal information is safeguarded. In other words, privacy management is no longer a value-added consideration, but also an expectation.

Under the old model, corporate professionals strove for compliance with privacy rules and regulations. Moving forward, the most successful enterprises will treat CI as valuable as any other intangible business asset. It is tied to goodwill, brand recognition, and customer satisfaction. Business professionals who consider privacy as a business issue – and not simply a compliance issue – will have a competitive advantage in the workplace. The management of CI is an operational risk, and as with all risks, these operations should be tailored to minimize losses.

PRIVACY MANAGEMENT PROGRAM

A well-executed Privacy Management Program (PMP) is preventative in nature. It seeks to eliminate the risk of mishandling CI by building protective measures into a company's existing technology and workflow. Not all companies will be ready to implement these changes. Companies who are in the business of risk management, such as investment firms or insurance companies, are more likely to make the transition. One key indicator of capacity and readiness is "task maturity" – an institution's ability to perform particular duties. As noted by Ken Anderson, former Assistant Commissioner for the Office of the Information and Privacy Commissioner of Ontario, "relatively mature organizations that have institutionalized risk management will discover, in many respects, that they can manage it as another area of risk, similar to those posed by technology, economic factors or the environment".[20]

A PMP system has benefits that extend beyond prevention. PMP systems allow an organization to comply with the existing legal and regulatory framework. It is evidence that a company has an internal set of checks and balances. It allows an organization to respond quickly to any external

[20] Privacy meets risk management, online: Information and Privacy Commissioner of Ontario <http://www.ipc.on.ca/images/Resources/2010-04-28-RIMS.pdf>.

audits, and defend itself against privacy complaints by customers or competitors. And it fosters a positive corporate image by demonstrating good will toward clients.

The first step toward a successful PMP is to identify privacy risks. Traditional risk identification processes, such as Privacy Impact Assessments (PIAs), have been used for decades as a formal risk management tool to identify potential or actual risks within a system, technology or process. For example, the Information and Privacy Commissioner of Ontario has set out Privacy Impact Assessment guidelines21 to assist health information custodians in reviewing the impact that a proposed information system, technology or program may have on the privacy of an individual's personal health information. A PIA can assess the following types of risk:

- Risks arising from a new technology or the convergence of existing technologies;
- Risks arising from the use of a known privacy-intrusive technology or practice in new circumstances, such as video surveillance or the recording of telephone conversations;
- Risks arising from a new program or from changing information handling practices; and,
- Risks arising from legacy systems that may not support privacy and security best practices. [22]

In addition to traditional risk identification processes, the following processes may also be used piecemeal, depending on the requirements of the particular organization[23]:

1. Develop a Culture of Privacy Protection – As mentioned earlier, embedding privacy into the existing processes and culture of an organization is a powerful way to prevent the mishandling of CI. In doing so, protection becomes second nature and part of a company's best practices.

2. Understand the flow of your organization's information – Most organizations are good at collecting and using CI, but fewer are adept at securely storing and destroying CI at the end of its life cycle. Fully documenting the entire process – including what is collected, who has access to it, where it is stored, and how it is accessed – is an important step in identifying risks. A complete inventory of original CI across the entire organization is a good starting point; however, many records are duplicated and used across different departments. For example, a paper record can be transcribed into a customer database, stored on IT servers, and disclosed to

[21] Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act , online: Information and Privacy Commissioner of Ontario <http://www.ipc.on.ca/images/Resources/phipa_pia-e.pdf>.

[22] Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act , online: Information and Privacy Commissioner of Ontario <http://www.ipc.on.ca/images/Resources/phipa_pia-e.pdf>.

[23] Privacy Risk Management: Building privacy protection into a Risk Management Framework to ensure that privacy risks are managed, by default . Online: Information and Privacy Commissioner of Ontario <http://www.ipc.on.ca/images/Resources/pbd-priv-risk-mgmt.pdf>.

third parties as part of an outsourcing agreement. Each instance of CI within an organization should be protected, regardless of medium or origin.

3. Examine Key Business Processes – Some areas of an organization warrant more attention than others. Sales, customer service, marketing and technical support are customer-facing and typically manage large quantities of CI. Often times, how information is first processed can determine whether a PMP is successful.

4. Assess the costs and risks associated with implementing a PMP – In order to minimize day-to-day operations, a cross-functional team should be assembled to identify potential roadblocks, privacy risks, and financial costs associated with implementation before any changes are actually made.

5. Review Third Party Processes – Many businesses outsource a variety of tasks to third party suppliers. Confidential CI may be transferred and stored off-site, and often times these third parties are outside the province or country. As a best practice, organizations should not outsource their accountability to protect confidential CI. In the unfortunate event that a supplier mishandles CI, the customer will still blame the outsourcing corporation. Therefore, businesses should work closely with third parties to manage their CI in a manner consistent with the organization's internal policies.

6. Appoint or hire a privacy officer or committee to oversee the privacy management program – While privacy protection should be the goal of every employee within an organization, a project of this magnitude may require dedicated effort and expertise. A privacy officer or committee would fill a variety of roles, including ensuring a smooth transition and company-wide compliance; working across departments and offices; engaging in regular internal audits; developing educational and training programs for employees; and acting as a liaison between employees and upper management to report on progress and suggest improvements.

7. Improving Security Measures – While more technical than process-oriented, an effective security system is vital to protect CI. Mature organizations should continue to strengthen their internal systems by finding gaps and weaknesses in existing infrastructure. Particular attention should be paid to the ways in which CI is inputted and exported from an organization's information management system.

WHAT SHOULD A PRIVACY OFFICER DO?

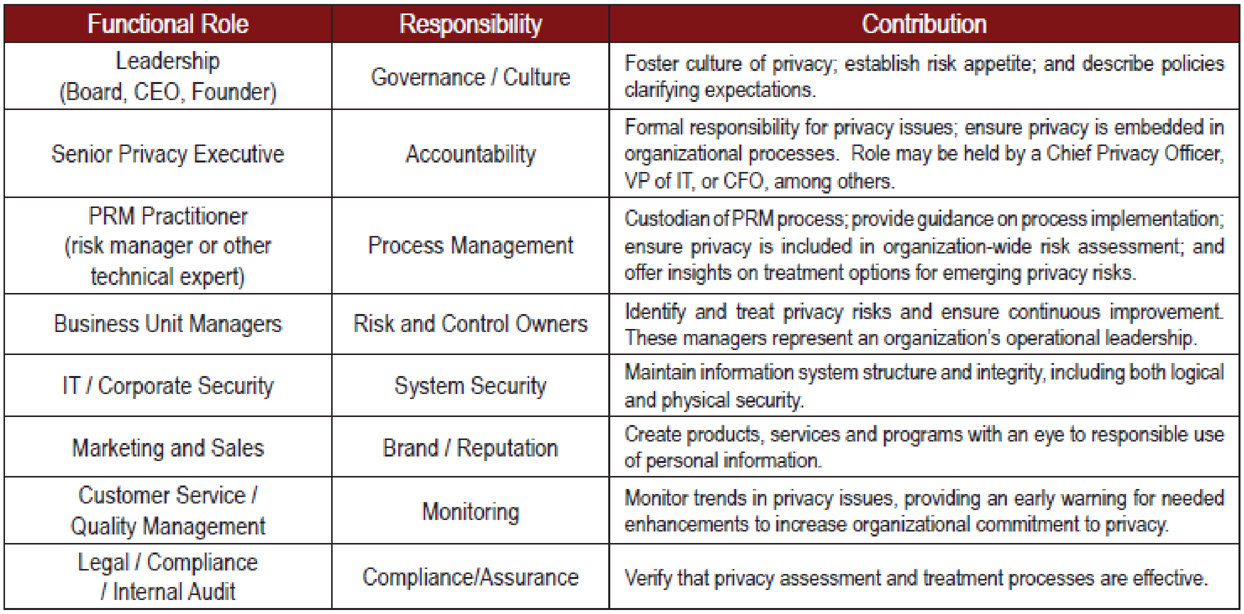
While identification and protection of CI is the responsibility of an entire organization, research suggests that individual employees tend not to consider privacy within their portfolio of responsibilities.[24] For instance, traditional risk managers are not trained or equipped to deal with modern privacy concerns, and IT managers see risk management through the narrow lens of their IT security practices. Part of the problem is the ill-defined scope of a privacy officer's responsibilities. He or she will play many roles, including the following:

- establish and implement internal reporting mechanisms to ensure that the right people know how the PMP functions and whether it is operating as expected;
- coordinate with other appropriate persons responsible for related disciplines and functions within the organization;
- develop educational and training programs for continuing education within the organization;
- be responsible for the ongoing assessment and revision of program controls;
- ensure compliance with applicable privacy legislation;
- represent the organization in the event of a complaint investigation by a privacy commissioner's office; and,
- advocate privacy within the organization itself.[25]

As a company's PMP matures, different and more sophisticated roles may be undertaken by various personnel:

[24] Privacy as a Risk Management Challenge for Corporate Practice, Ted Rogers School of Management, Ryerson University, online: <http://ryerson.ca/content/dam/tedrogersschool/privacy/privacy_as_a_risk_management_challenge.pdf>.

[25] Getting Accountability Right with a Privacy Management Program , online: Office of the Privacy Commissioner of Canada <https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp>.



Functional Role	Responsibility	Contribution
Leadership (Board, CEO, Founder)	Governance / Culture	Foster culture of privacy; establish risk appetite; and describe policies clarifying expectations.
Senior Privacy Executive	Accountability	Formal responsibility for privacy issues; ensure privacy is embedded in organizational processes. Role may be held by a Chief Privacy Officer, VP of IT, or CFO, among others.
PRM Practitioner (risk manager or other technical expert)	Process Management	Custodian of PRM process; provide guidance on process implementation; ensure privacy is included in organization-wide risk assessment; and offer insights on treatment options for emerging privacy risks.
Business Unit Managers	Risk and Control Owners	Identify and treat privacy risks and ensure continuous improvement. These managers represent an organization's operational leadership.
IT / Corporate Security	System Security	Maintain information system structure and integrity, including both logical and physical security.
Marketing and Sales	Brand / Reputation	Create products, services and programs with an eye to responsible use of personal information.
Customer Service / Quality Management	Monitoring	Monitor trends in privacy issues, providing an early warning for needed enhancements to increase organizational commitment to privacy.
Legal / Compliance / Internal Audit	Compliance/Assurance	Verify that privacy assessment and treatment processes are effective.

Possible PMP roles and contributions[26]

The effect of a comprehensive training and educational program cannot be understated. Human error is one of the most common causes of reported organizational breaches.[27] Examples include misdirected mail and faxes; e-mail addresses viewable in mass e-mails; inappropriate disposal of documents; and improper disclosure of passwords.[28]

Employees will be better equipped to protect privacy when they are able to recognize potential breaches before they occur. Education and training can be delivered in many ways, including company-wide conference calls, online training modules, or departmental training sessions.

For privacy training and education to be effective, it must:

- be mandatory for all new employees before they access personal information and periodically thereafter;
- cover the policies and procedures established by the organization;
- be delivered in the most appropriate and effective manner, based on organizational needs; and,

[26] Privacy Risk Management: Building privacy protection into a Risk Management Framework to ensure that privacy risks are managed, by default . Online: Information and Privacy Commissioner of Ontario <http://www.ipc.on.ca/images/Resources/pbd-priv-risk-mgmt.pdf>.

[27] Getting Accountability Right with a Privacy Management Program , online: Office of the Privacy Commissioner of Canada <https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp>.asp

[28] Getting Accountability Right with a Privacy Management Program , online: Office of the Privacy Commissioner of Canada <https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp>.

• circulate essential information to relevant employees as soon as practical if an urgent need arises.[29]

CONSIDER THIRD PARTY SUPPORT AND EXPERTISE

Organizations that cannot spare the personnel, do not have the expertise, or have limited funds may consider outside support to deliver piecemeal or wholesale PMP-related services. Cybersecurity is a growing industry, and many corporations have emerged to fill the demand. Some organizations specialize in providing rapid emergency response to data breaches, while others focus on initial risk assessments and tailoring PMPs to fit specific business needs. Some of these security companies also provide sophisticated forensic services that track and recover lost or stolen data, and collect and analyze mobile GPS signals and other transmissions. Such services can allow corporations to rapidly implement a PMP system to comply with customer and regulatory demands, and to react quickly to data breaches or external threats.

CONCLUSION

Risk management plays a vital and multi-faceted role in the successful handling of customer information. Privacy has become paramount in the minds of consumers, and thus must be treated with the same strategic initiative as other conventional business processes. An effective risk management strategy is key to ensuring that companies have a structured and effective approach to respond to emerging privacy, legal, and security issues.

HELPFUL RESOURCES

Information and Privacy Commissioner of Ontario

Privacy Risk Management: Building privacy protection into a Risk Management Framework to ensure that privacy risks are managed, by default <http://www.ipc.on.ca/images/Resources/pbd-priv-risk-mgmt.pdf>.

Privacy meets risk management <http://www.ipc.on.ca/images/Resources/2010-04-28-RIMS.pdf>.

Privacy Impact Assessment Guidelines for the Ontario Personal Health Information Protection Act <http://www.ipc.on.ca/images/Resources/phipa_pia-e.pdf>

[29] Getting Accountability Right with a Privacy Management Program , online: Office of the Privacy Commissioner of Canada <https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp>.

International Organization for Standardization

The risk management toolbox
<http://www.iso.org/iso/home/news_index/news_archive/news.htm?Refid=Ref1586>

Office of the Privacy Commissioner of Canada

Getting Accountability Right with a Privacy Management Program
<https://www.priv.gc.ca/information/guide/2012/gl_acc_201204_e.asp>.

Privacy Toolkit: A Guide for Businesses and Organizations
<http://www.priv.gc.ca/information/pub/guide_org_e.asp>

Office of The Superintendent of Financial Institutions Canada

Cyber Security Self-Assessment Guidance <http://www.osfi-bsif.gc.ca/Eng/Docs/cbrsk.pdf>

Ponemon Institute

Exposing the Cybersecurity Cracks: A Global Perspective (2014)
<http://www.websense.com/assets/reports/report-ponemon-2014-exposing-cybersecurity-cracks-en.pdf>.

Ted Rogers School of Management, Ryerson University

Privacy as a Risk Management Challenge for Corporate Practice
<http://ryerson.ca/content/dam/tedrogersschool/privacy/privacy_as_a_risk_management_challenge.pdf>.