OPC Incident Reporting Research

Report to the Office of the Privacy Commissioner of Canada

Nymity Inc.
Brookfield Place
161 Bay Street, 26th Floor
Toronto, ON
M5J 2S1

Main: 416 572 2777
Toll-Free: 866 3NYMITY

Email: info@nymity.com

Nymity Inc.
245 Park Avenue
39th Floor
New York City, NY
10167

Nymity Inc.
Berkeley Square House
2nd Floor
Berkeley Square
London, England
W1J 6BD

Table of Contents

1. Executive Summary

1.1 Background

For almost 2 years now, the Office of the Privacy Commissioner of Canada (OPC) has been encouraging private-sector organizations who have experienced a breach of security of their personal information holdings to report such breaches to the OPC. This voluntary reporting regime was detailed in guidelines published by the OPC in August 2007, titled "Key Steps for Organizations in Responding to Privacy Breaches" [1](the 'Guidelines'). In Step 3: Notification, section (iv) Others to Contact, the Guidelines outline the specific detail for such reporting and provide that "organizations are encouraged to report material privacy breaches to the appropriate privacy commissioner(s)."

The Guidelines provide a number of factors that organizations are to consider in determining whether a breach is material and therefore subject to the voluntary reporting guideline. These factors include:

- any applicable legislation that may require notification;
- if the personal information is subject to privacy legislation;
- the type of personal information affected, including:
    - if the information could be used for identity theft
    - if there was a reasonable chance of harm, including non-monetary losses.
- the number of individuals affected;
- whether affected individuals have been notified; and
- if the commissioner's office might receive complaints or inquiries relating to the breach.

In its Guidelines the OPC noted that it was encouraging organizations to report breaches for the following purposes:

- to help the OPC respond to inquiries made by the public and to respond to any complaints it may receive; and
- so that the OPC may provide advice or guidance to the organization that may be helpful in responding to the breach.

1.2 Study Purpose and Objective

The OPC initiated the OPC Incident Reporting Research project with a view to understanding the impediments to reporting breaches to the OPC within the current voluntary reporting regime, and to gain an understanding of the potential impact that the proposed mandatory breach reporting amendments to the *Personal Information Protection and Electronic Documents Act* (PIPEDA) will have on organizations that are subject to PIPEDA.

[1] http://www.priv.gc.ca/information/guide/2007/gl_070801_02_e.cfm

During the period between January 1, 2006 and December 31, 2008, the OPC recorded a total of 136 breaches. Of those, 113[2] incidents (83.1%) were self-reported by the organizations responsible. One of the objectives of this research project is to determine if the quantity of breach incidents was representative of the number of breaches occurring within private-sector companies or if there existed a hesitancy to report material breaches resulting in significant numbers of them being unreported to the OPC.

1.3 Key Findings

Voluntary Reporting

Private-sector organizations have a good awareness of the Guidelines issued by the OPC. Almost all respondents were conversant with the intent and content of the Guidelines, and this was particularly noticeable when organizations described their breach response processes. Many organizations have structured their processes based on the OPC Guidelines, and when asked what factors are considered when deciding whether or not to report a breach, the majority referenced the factors identified in the Guidelines.

Human error is a key underlying root cause in many of the breach incidents that respondents reported in the survey. However, system "glitches" such as envelope stuffing, inappropriate access by employees, and lost hardware were also cited sources of privacy breach incidents.

When faced with a privacy incident and the need to make a decision whether or not to report the incident to the OPC, the majority of the respondents quoted verbatim the factors to be considered contained in the Guidelines. In determining whether to report, respondents noted the key factors considered were typically the sensitivity of the information affected, the number of individuals affected, and the likelihood of the breach becoming public knowledge either to the OPC via a complaint or through the media.

There is a strong acceptance of the OPC's current voluntary reporting regime, and during our interviews we did not sense much resistance to reporting. The challenge for organizations lies in determining how the factors to consider related to each other. Organizations are seeking some clarity as to the definitions, with some examples of when, and when not, the OPC would expect organizations to report an incident.

To encourage reporting within a voluntary reporting regime, organizations are looking to the OPC to provide some additional information as to what the OPC does with the information it receives. Over a quarter of the respondents felt that since reporting is voluntary it should never result in an investigation.

[2] 17 of the 113 incidents were self-reported regarding the same incident at the urging of a credit agency.

Organizations were also concerned about any publicity arising from reporting, noting that since the reporting is voluntary the organization's name should not be publicized by the OPC.

Mandatory Reporting

Although organizations did not express significant opposition to reporting incidents to the OPC, the fact that such reporting may become mandatory created concerns for organizations. The most common concern related to the potential penalties that might result from not reporting when required to do so. As the definition of "material" contained in the Industry Canada framework still requires organizations to "consider" a number of factors, a differing interpretation of those factors may result in non-compliance, potentially leading to penalties. In this context almost one-third of the respondents asked for the OPC to develop more specific interpretive documents to help organizations interpret terms such as "sensitivity of the information," "number of individuals affected," and "significant harm."

Respondents also identified some of the ways that implementation of a mandatory reporting regime may affect their organization. Many respondents identified both positive impacts and negative impact. On the positive side, a number of participants noted that mandatory reporting may bring more focus and discipline to their policies and prevention of breaches. On the negative side, almost a quarter of respondents noted that mandatory reporting may create additional expense (for example, from the need to add staff to the privacy office or the use of legal counsel to provide assistance in dealing with the new reporting requirement).

Ninety-six percent of respondents reported that they did not anticipate any significant change in the overall number of breaches reported to the OPC, based on the proposed Industry Canada framework and their own internal decision-making process based on the current Guidelines.

When asked if reporting anonymously to a third party would affect an organization's decision to report a breach incident, almost 60% of respondents stated they were not in favour of this option and would prefer to report directly to the OPC.

Privacy Management Programs

To date, companies have by and large not initiated any specific actions to prepare for mandatory reporting. Most organizations seem to be taking a "wait and see" attitude, waiting until further action is taken before investing any resources. Training was by far the most often-mentioned initiative being considered, if a mandatory reporting requirement was to be passed.
Just over half of the respondents reported that their organization had a formal, documented breach protocol in place. The remaining half was not

without some form of breach response plan, but they tended to be much more informal, often relying on the experience and expertise of the privacy office or Privacy Officer. Most of the survey participants, whether they had a formally documented protocol or not, used the structure of the Guidelines as a tool to respond to breach incidents.

When participants were asked to rate the overall maturity of their organization's overall privacy management program on a scale of 1 to 10 (with 10 being fully mature and complete) the largest grouping (33%) rated their program as 8/9. Another 33% rated the maturity of their privacy management program as either 5/6 or 6/7. Those at the lower end of the scale generally stated that they had basic policies in place, had a privacy notice on their website, and had done some training, but fully recognized that more work had to be done.

Participants also provided input about initiatives that were either being implemented or under consideration for implementation during 2010 and 2011. Almost 6 out 10 companies (59%) are planning additional training and awareness programs over the next two years. The next most often-mentioned initiatives were:

- creating/updating data retention policies;
- reviewing third-party contracts and performing third-party audits;
- implementing encryption;
- auditing current practices and doing a gap analysis;
- installing logging/tracking software;
- creating/updating overall records management programs; and
- protecting mobile devices.

2. Voluntary Reporting

The first part of the study sought to determine how organizations are interacting with the current voluntary incident reporting Guidelines. As part of the basis for initiating the research project, the OPC noted that the statistical data it had collected regarding incidents did not provide any information relating to whether organizations were reporting all material breaches and if the relatively small number of reported incidents was representative of the fact that organizations were not experiencing large numbers of breaches. Alternatively, the small number of reported incidents may mean that Canadian organizations are not reporting breach incidents when in fact the actual number of breaches is significantly larger than the numbers reported. The OPC noted that U.S. studies seem to indicate that U.S. companies were experiencing significantly more breaches than were being reported by Canadian companies.

2.1 Awareness

The study found that all 27 organizations contacted were aware of the existence and the general content of the Guidelines. The vast majority of respondents indicated a very high level of awareness of the requirements of the OPC Guidelines, although a small number acknowledged that they were not as familiar with the details as they likely should be.

Question:

Are you/Is your organization aware of the current voluntary breach reporting guidelines, and how they apply to your organization?

When asked how they became aware of the Guidelines, participants noted some of the following sources[3]:

- Nymity's daily alerts;
- directly from the OPC website;
- industry associations;
- as a result of having participated in the consultation process to develop the Guidelines; and
- others, such as legal briefs, conferences, media.

2.2 Common Sources of Breach Incidents

Survey participants were asked to identify the most common root causes of their breach incidents. The most common sources of breaches were as a result of human error. Slightly more than half of all

Question:

In the past has your organization experienced any incidents where personal information was lost or inappropriately used or disclosed? If so, please describe the nature or source of the incident.

[3] Listed in order of mention; some participants indicated more than one source

incidents (51%) resulted from employee errors. Examples provided by respondents included:

- "a customer representative sent an email to the wrong recipient by inadvertently typing the wrong email address in the To: line";
- "a form containing personal information was sent to the wrong individual when an employee input the incorrect house number into the address field";
- "we exposed other recipients' email addresses in the 'to' line of an email by not properly using the 'bcc' function as required";
- "we sent a fax to the wrong company in error";
- "we did not completely scrub a hard drive returned to us by one customer before selling it to another customer".

While most of the employee-caused breaches could be characterized as human error, a small number of respondents noted that the inappropriate use or disclosure in some occasions was deliberate. One participant noted that an employee "collected information about our customers and then used that information to solicit customers for a business the employee was operating on the side," while another respondent noted that "employees sometimes like to look at other people's information, such as friends, family or even ex-spouses, often for purposes related to broken relationships."

The second most common cause, 26% of reported incidents, is the loss of hardware, including laptops, portable storage devices, and other storage media. It is important to note that many organizations identified stolen/lost laptops as a security incident[4], but in those cases where the laptop was protected by means of encryption[5], the matter was not considered to be a loss of personal information.

A review of the incidents by industry found that in the telecommunications, financial, and insurance sectors, where billing is still commonly done by mail, incidents of incorrect envelope stuffing was a concern and represented 18% of incidents. A number of organizations in these industry sectors reported that they had processes in place to audit envelope stuffing, and that the incidents, which were generally limited to small numbers of customers, usually resulted in customers being contacted and advised of the error.

It is interesting to note that an overwhelming majority of breaches reported by survey participants related to internal processes; only 2 organizations reported any situation relating to an external breach, such as access to a database by an external source. One participant reported that inadvertently

[4] Some organizations created a distinction between security incidents—a loss of hardware or inappropriate access to a premises—and privacy incidents (where personal information is involved). It was noted that a security incident can result in a privacy incident but for security incidents, the initial investigation often does not involve the Privacy Officer unless the investigation by the Security team identifies that personal information may have been involved.

[5] A number of organizations noted that they have installed full-disk encryption on laptops and other mobile devices. Others indicated that implementing encryption is an initiative planned within the next two years.

"a database containing personal information was accessible to unauthorized individuals via the Internet."

Four (4) organizations (15% of all respondents) reported that they have not had any incidents involving a loss or inappropriate access or use of personal information.[6]

Although employee personal information is not subject to PIPEDA (unless the organization meets the definition of federal work, undertaking, or business), companies considered incidents involving employee personal information as breaches for the purpose of reporting to the OPC. As noted by one participant, "employees may not be covered, but we treat our employees' information exactly the same as we treat our customers'; we don't see any distinction between the two."

2.3 Breach Incident Detection

Most of the participating organizations have developed processes that are designed to identify, report, and address privacy breaches. Ninety-three percent (93%) of respondents have developed some form of process that may include specific hard-copy forms or system templates that record the nature of the incident, and a formal escalation process that generally commences in a customer service area, includes business management where appropriate and escalates to the organization's Privacy Office/Privacy Officer.

The depth and breadth of these policies are generally commensurate with the size of the organization: large organizations generally reported more detailed and often mechanized processes that are fully documented; smaller organizations often relied more on paper and email escalation processes and often relied on the experience and knowledge of the Privacy Officer rather than formalized documented procedures.

As explained by one participant, the organization "has a rigorous complaint-handling process which has the ability to flag all privacy related inquiries—simply ticking a "privacy" box on the system triggers a note to the privacy compliance expert in the relevant line of business. All privacy issues are immediately rated as low, medium, or high, which determines the level of escalation required."

A participant in a medium-sized organization noted that it "is a challenge sometimes to have everyone recognize a privacy issue when it comes up" and therefore not every issue may be identified and escalated as required.
The majority of respondents expressed a level of confidence that, in the case where an employee may have triggered a potential incident (such as sending

[6] Of the four organizations that reported no breaches it is noted that three of these organizations do not have a formal breach response plan in place, either having no plan at all or only informal processes.

an email to the wrong recipient), the employee would self-report the incident as required under the policy. Many organizations felt that their employees were confident that in the case of human error, the employer was more interested in resolving the customer/privacy issue than in punishing the employee, thereby encouraging reporting. One organization noted that it had implemented penalties for employees who fail to report incidents where the policy required such reporting.

2.4 How the Decision to Report to the OPC is Made

The decision on whether to report or not report an incident to the OPC is one that organizations carefully consider as part of the overall breach response process.

Questions:

When it is determined that a breach of PI has occurred how is the decision to notify the OPC made?

Under what circumstances would the OPC be notified?

Generally, those organizations in industries which are subject to other regulatory bodies, for example, financial services and telecommunication companies, were more likely to support voluntary reporting to the OPC. Only one organization reported that it would not report any breach to the OPC unless such reporting was mandatory. It noted that "there is no legal obligation to report, it doesn't provide any benefits but only creates a potential liability, such as an investigation."

Although there may have been differences expressed as to the "desirability" of self-reporting, the vast majority indicated that they were aligned with the objectives and purposes of reporting, which is to provide assistance to the reporting organization and provide proactive awareness for the OPC in the event of a complaint or media attention. It is clear from participants' responses that those organizations and/or privacy professionals who have a strong working relationship with the OPC were generally more favourable to self-reporting, and the fact that a climate of mutual respect existed was encouraging to those respondents. As one participant stated, "the Privacy Commissioner has been very supportive and understands the business issues—the OPC has always provided good feedback to help us resolve the issue at hand."

Participants who had no or minimal contact with the OPC were generally more reluctant to self-report, as one participant noted, "I'm not sure what they do with the information and in the middle of a breach the last thing I need is to be distracted by someone telling us what to do."

The study identified that although organizations are mostly supportive of voluntary self-reporting, there is continued concern about what the OPC does with this information. A number of common concerns expressed included:

- Will each report trigger an investigation by the OPC?

- When should the report be provided?
    - Reporting too early may result in a report that is incomplete and cause additional interactions with the OPC, potentially distracting from remediation efforts.
- How long will the OPC retain the information? For example, if a large organization has a number of relatively small breaches over a period of time will frequency result in an audit or investigation.
- Will the OPC publicize the incidents reported by organizations?
- Will other organizations be able to obtain the information voluntarily reported to the OPC and use that information for other purposes, such as reporting to the press?

In many organizations the decision to self-report is made by the Privacy Officer. Often, the team responsible for investigating and managing the incident—which typically includes representatives of the business channel in which the breach occurred, Information Technology (IT), internal compliance or security, and the privacy office/Privacy Officer—created a recommendation to report or not report. The final decision in many cases was left to the discretion of the Privacy Officer, although in some organizations the decision was taken after consultation with a C-level executive such as the Chief Legal Officer, Chief Compliance Office or Chief Financial Officer. Only in smaller organizations would the CEO be involved in this decision.

It was obvious from participants' responses that the OPC Guidelines were well-read and understood. To determine if the OPC should be notified of a breach, organizations reported that they considered many of the same factors that were outlined in the Guidelines, including factors such as:

- number of individuals affected;
- types/nature of information affected, for example:
    - sensitivity;
    - how much information is affected.
- likelihood of complaint to OPC;
- likelihood of becoming public knowledge;
- if affected parties were notified;
- requirements under any contracts or agreements;
- how significant is the risk of harm in the context of the information affected;
- whether the incident is a "one-off" versus a trend.

A number of organizations noted that they would only report to the OPC if the customer was notified—they could not envision any situation where the OPC may be notified without notifying affected individuals. As one individual noted, "if it does not warrant notifying customers as the information was not sensitive or there was no risk of harm, why would the OPC want to know?"

Many of the larger organizations have created a structured incident ranking process whereby incidents are ranked according to seriousness. For example,

one organization described its classification system, which uses a rating of seriousness using a numerical number scheme from #1 to #3, as follows: a #3 incident is where sensitive personal information of a large number of parties is affected, a #2 incident may affect a significant number but only affects names or basic contact information within a low-risk context, and a #1 incident may be a one-off email note sent to the wrong individual. Other organizations have used terminology such as “high, medium or low risk” to classify incidents. The organizations usually predetermine that all #3 or “high risk” incidents will automatically be reported, #2 or “medium risk” incidents are only reported if the context leans in favour of reporting, and #1 or “low risk” incidents are never reported.

Although reporting is very much considered the “right thing to do,” it is obvious that organizations continue to struggle with the practical application of the Guidelines. The relationship between all of these factors is very contextual and therefore no one factor by itself seemed to override the others.

Some examples that highlight these challenges include the following:

- Company A noted that “if it exposed the email addresses of twenty customers in an email header, it would likely not report the incident as an email address is generally not sensitive. However, if it exposed the bank account or credit card numbers of twenty customers it would likely self-report”;
- Company B reported that “a box containing unencrypted storage tapes was inadvertently taken to the dump and discarded—although the tapes contained personal information of a large number of people, the likelihood of it being misused was deemed to be very low so should it be reported?”;
- Company C reported a situation where “due to an envelope stuffing error, over 100 envelopes were sent to the wrong customers—although customers were all contacted, it may not be self-reportable as 100 envelopes is a very small number since the monthly mail-out can be as large as 10 million envelopes—therefore the error rate is within normal operating tolerances”;
- Company D noted that it had “discovered a breach of fairly sensitive information of a reasonably large number of individuals but the breach occurred several years ago—does the long time between the event and its discovery affect the need to report?”
- Company E did not report an incident that it had initially identified internally as “severe” noting that “we deemed it be severe as it was not immediately clear what had happened, a third party was hired to fix the problem, but in the end it only affected a small number of individuals, no sensitive data was affected, and in fact, we were not even sure a breach had occurred.”

Some organizations also struggle with the nuances between privacy incidents and privacy breaches. For example, if an envelope is sent to a customer at the last address provided by the customer and they have subsequently moved and the new homeowner returns the envelope unopened, is this considered a privacy incident or a breach? If the new homeowner opened the envelope and then returned it, is this a privacy breach or an incident?

One participant reported that a laptop was stolen, which contained the personal information of less than 70 individuals. They stated that "we notified all the affected parties and although the information affected was non-public information, none of the customers complained or felt the information was "sensitive" so the incident was not reported to the OPC—we based the decision on the number of individuals and the degree of sensitivity of the information."

In spite of the above concerns, it is fair to characterize the overall acceptance of voluntary reporting as favourable, and that there does not appear to be a climate of significant resistance to voluntary reporting today.

2.5 Interaction with the Privacy Commissioner's Office

Participants who have self-reported incidents in the past were asked to provide some input regarding the process of self-reporting and the response(s) it received from the OPC.

Question:

If a breach has been reported to the OPC, how would you describe the overall experience?

Six (6) respondents stated that their organizations had self-reported to the OPC one or more breach incidents which they believed met the criteria as detailed in the Guidelines. The respondents rated the overall experience as positive, with 2 respondents describing the experience as "extremely" or "very" positive, 3 describing the experience as positive, and one respondent reporting that the experience was "mixed."

Those who rated the overall experience as positive provided the following comments:

- "the OPC understood the realities of the situation and were extremely focused on what had been done to stop the situation, what was done to assist the customer, and what measures had been taken to prevent it from happening again";
- "the OPC was supportive and not dogmatic."

Some additional comments noted that:

- "it can take a while to get a response from the OPC":
  - one company stated that 3 months after reporting an incident it received a call back from the OPC with some additional

questions—after that length of time some of the data may not be readily available.

- "organizations would appreciate a final letter noting that the report had been received and that the file had been closed";
- "there needs to be a consistent response from provincial and federal privacy commissioners":
    - one company who reported an incident to multiple commissioners received positive feedback on its actions from two provincial privacy commissioners, however, the OPC was somewhat critical of the company's actions.

2.6 How to Encourage Voluntary Reporting

Survey participants were asked to identify any actions, incentives, or support processes that the OPC could put in place to encourage voluntary reporting.

Questions:

What actions or incentives can the OPC put in place to encourage reporting of breaches?

What support process can be provided by the OPC that will facilitate voluntary reporting to the OPC?

Although very few organizations commented on the actual process of reporting, indicating that the process itself is satisfactory, there was considerable input on the things that the OPC can do to ease concerns and encourage self-reporting.

Twenty-seven percent (27%) of respondents strongly felt that since reporting is voluntary, no investigations should be undertaken as a result of that reporting. If the purpose of reporting is to assist organizations in dealing with the breach incident and to be prepared in the event of a complaint or media inquiry, than no investigation should be initiated from the report, absent a specific complaint.

Confidentiality was top of mind for a number of respondents. Eighteen percent (18%) of respondents commented on matters relating to keeping the name of the reporting company confidential and ensuring that company names are not used in any reports issued by the OPC. As one participant stated, "if we have made all of our customers happy and have taken steps to make sure it doesn't happen again, we shouldn't be subjected to name and shame—leave that for others who are not prepared to do the right thing." Or as another participant put it, "making public the names of companies that are doing the right thing by self-reporting seems like a disincentive to report." Although a small number of participants suggested that the OPC consider anonymous reporting, as we will see in Section 3.6, this idea was not supported by the majority of respondents.

The majority of respondents encouraged the OPC to provide organizations with more information regarding what is done with the information collected

by means of reporting, and by doing so, more effectively create a sense of "comfort" that the OPC intends to work together with organizations. Communication with organizations should be focused on providing assistance to mitigate harm and prevent future breaches. One respondent noted that "the focus of reports to the OPC and the subsequent discussions should not be on what happened, but much more importantly, on what steps the organization has taken to strengthen security, mitigate harm, and improve overall privacy."

However, in what seemingly is a conflict with the "confidentially" issue discussed above, one participant went so far as to suggest that the OPC "should publicly name organizations that went 'over and above' in their response to a privacy breach incident."

From a process perspective, respondents had the following input:

- better explain the thresholds for reporting, i.e. what is material, by providing examples of specific situations that would or would not trigger voluntary reporting;
- provide support on what, when, and how to report incidents by means of a list of frequently asked questions (FAQs);
- for each reported incident, assign one individual within the OPC to liaise with the organization—ensures consistency and builds relationships;
- provide a fill-in-the-blank form on the OPC website for ease of reporting.

3. Mandatory Reporting

The second part of this study sought to discover organizations' opinion about the proposed amendments to PIPEDA relating to a mandatory requirement to report incidents to the Privacy Commissioner's office. Participants were provided with an overview of the mandatory reporting framework as developed by Industry Canada in its roundtable stakeholder consultations.

3.1 Will Mandatory Reporting Affect the Decision Making Process?

As the framework proposed by Industry Canada includes a new element into the definition of materiality, the study asked organizations how a mandatory reporting requirement might affect the decision making process compared to the decision making process under a voluntary regime.

Questions:

Based on the proposed framework, has your organization experienced any data-loss incidents in the past that were not reported to the OPC that would be reportable now?

Under a mandatory reporting regime, would the process to decide on when to report be different than it is today?

When asked if a previously unreported incident would have been reportable under a mandatory regime eighty-nine percent (89%) of respondents indicated that the incident would still be not reportable under the proposed framework. The remaining eleven percent (11%) stated the new framework may have potentially changed the decision.

One of the new factors to be considered is "whether the data breach constitutes a pattern, or provides evidence of a systemic root-cause outside of commercially acceptable operating standards." Some organizations noted that this element lacks clarity. This could result in more breach incidents being reported. For example, if over the period of a year a number of emails are sent to the wrong recipients due to simply mistyping an email address, would this constitute a pattern? On the other hand, if during one month a large number of envelopes are sent to wrong addresses—for example 500 misdirected out of 5 million sent—is this error rate within acceptable operating standards?

Sixty-three percent (63%) of respondents indicated that their decision making process would not change in any way under a mandatory regime. For those organizations who reported some potential change to the decision making process, the most common change was earlier or deeper participation in the process by legal counsel, both internal and external. As described by one participant, "if this becomes a legal requirement then our counsel will want to sign off on when, why, and what we are reporting, as

there is now a liability that did not exist before." A number of respondents noted additional rigour may be added to the decision making process to ensure compliance, while others noted that the final decision sign-off may occur higher up the organization, for example, by Legal or a C-level executive. A number of respondents indicated this new requirement may increase accountability for the business channels, as one participant noted, "this will put more onus on the business folks; they need to be on board to prevent breaches from happening."

3.2 Impact on Organizations

Respondents identified a number of ways that mandatory reporting may affect their organization.

Question:

What impact do you believe that mandatory reporting will have on your company?

Twenty-two percent (22%) of respondents indicated that mandatory reporting would not have any impact on their company.

Of the seventy-eight percent (78%) who identified potential impact, they expected an equal amount of positive and negative impact.

Positive impact identified:

- company to develop a structured reporting policy or matrix: 27%;
- creates additional awareness of privacy overall: 27%;
- focuses the company on prevention: 18%; and
- puts more accountability for privacy into the business channels: 11%.

Other comments by respondents included that mandatory reporting will:

- "strengthen the role of the Privacy Office within the company";
- "result in more formal disciplinary action against employees who knowingly cause privacy breaches";
- "provide an opportunity to get more 'face time' with senior management and peers—I'm going to exploit this chance to go out and preach the gospel."

The negative impact resulting from mandatory reporting was generally driven by costs. Respondents noted the following potential sources of additional expense to deal with mandatory reporting:

- costs associated with a more rigorous decision making process, for example, use of outside legal counsel: 26%;
- additional staffing within the Privacy Office: 22%;
- training costs: 11%.

One company noted that to ensure compliance it would likely add privacy as a component to the annual corporate governance audit performed by its external auditors.

3.3 Reporting Trends

Respondents were asked to identify the impact that mandatory reporting would have on the number of incidents that would be reported internally to the Privacy Office and/or Privacy Officer, and the number of incidents that would be reported to the OPC.

Internal reporting:

The majority of respondents (70%) felt that after mandatory reporting requirements come into effect, the number of incidents reported up to the Privacy Office or Privacy Officer would not change. In general they felt that their current privacy program was sufficiently robust to ensure that any suspected privacy breach would already be reported up through the organization.

Question:

Estimate the number of incidents reported to the Privacy Office/Privacy Officer in 2008 and how many would be anticipated after mandatory reporting.

However, twenty-six (26%) of respondents felt that mandatory reporting obligations would increase the overall number of incidents reported to the Privacy Office or Privacy Officer. Although the majority of these anticipated a "slight" increase over time, one participant stated that "if a company was planning any training or awareness campaigns, it should expect a one-time surge in the number of incidents reported to the Privacy Office or Privacy Officer," and noted that when it did some training, it had "a spike in the number of incidents reported—at least a 25% increase for a while and then it settled down again."

From statistics provided by respondents, we noted the following trends:

- large, multi-branch organizations, such as financial institutions and retailers, were more likely to record larger numbers of incidents, however, they generally involved minimal sensitive data and were usually caused by human error;
- the more robust and highly structured the organization's privacy management program, the more incidents were reported to the Privacy Office or Privacy Officer.

Reporting to the OPC:

Ninety-six percent (96%) of respondents reported that, based on the proposed Industry Canada framework and their own internal decision making process based on the current Guidelines, there would be no change in the overall number of breach incidents reported to the OPC.

Question:

Estimate the number incidents reported to the OPC and how many would be anticipated after mandatory reporting.

Respondents generally felt comfortable that decisions taken to date to report or not report were still appropriate within the proposed framework. A number of organizations added commentary relating to how the framework, if adopted as is, may be interpreted and how this may affect future reporting. As further discussed below, it was evident from the commentary that over-reporting was a concern but something that could be managed and tempered by effective guidelines and examples from the OPC.

3.4 Concerns Arising from Mandatory Reporting

Question:

Are there any concerns created by the mandatory reporting of breaches to the OPC and why?

Although organizations did not express significant opposition to reporting incidents to the OPC, the fact that such reporting may become mandatory did create concern for organizations.

One-third of companies reported that mandatory reporting, rather than voluntary reporting, caused no additional concerns. These companies felt that their policies and processes were such that they would withstand any additional scrutiny that may result from a mandatory reporting regime.

The other two-thirds of participants identified a number of new or heightened concerns raised by mandatory reporting. The most common issue raised (by 26% of participants) was related to the potential penalties or liability that might arise if organizations did not report as required. The issue here was not that they would not report at all, but that the definition of "materiality" may be open to interpretation, and if the OPC's definition of materiality is not clear and concise, then organizations face an unreasonable risk of inadvertent non-compliance. As one respondent noted under the voluntary reporting regime, "we may have a difference of opinion with the OPC whether an incident should have been reported, but now there is a risk of liability associated with that differing opinion." The corollary is that organizations may thus over-report, a concern expressed by almost 20% of respondents, creating a negative impact for both reporting organizations and the OPC (who will be required to process and manage an increased flow of incident reports).

A number of organizations, particularly those in regulated industries, expressed concern that an overlap may exist between regulators. In some industries, organizations are required to report to regulators any information that may be "material." The concern was raised that if an organization had a breach that met the definition of "material" as described in the Industry Canada framework, although it may not be material to the business, it may in fact prompt an additional requirement to report the privacy incident to the industry regulator and/or prompt an additional investigation by that regulator.

Almost twenty percent (20%) of respondents expressed concern about how the OPC may choose to make public breach incidents, especially if the breach was not widely known.

3.5 Factors to Encourage and Support Mandatory Reporting

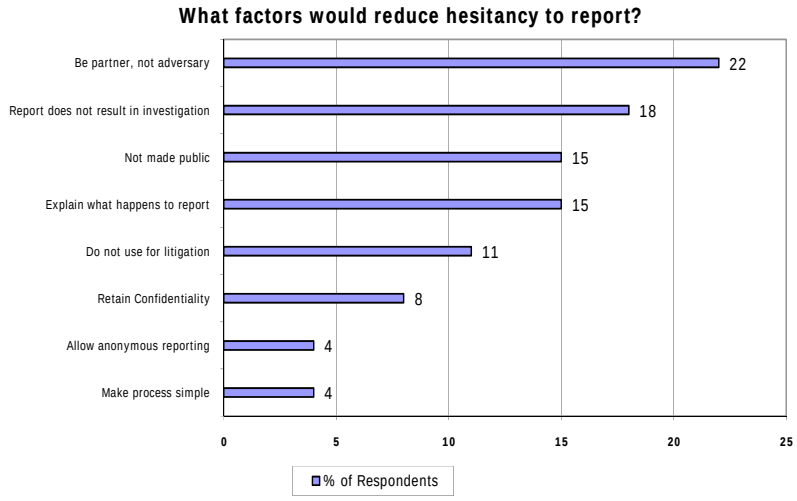
The survey posed two questions relating to how the OPC can assist organizations in meeting the proposed mandatory requirements.

Questions:

What factors would reduce any hesitancy to report?

If/when reporting becomes mandatory, what support do you need to assist you in conforming to the new requirements?

In response to the question relating to how the OPC can reduce any hesitancy to report, the number one response, from twenty-two percent (22%) of the respondents was that the OPC must be a "partner" and not be seen in a "policing" or "adversarial" role. Eighteen percent (18%) of respondents noted that the OPC needed to assure organizations that not every report would result in an investigation. Other factors noted were that the OPC would not make reports public (15%), the OPC should explain to organizations what would happen with the reports once received, and assure organizations that the reports would not be used as a basis for legal action against the company. The chart below lists all of the answers provided to this question.



When asked what support organizations needed, the largest number of respondents asked for the OPC to develop more specific guidelines to better assist them in interpreting the requirements. Almost 30% of respondents asked for detailed examples on how to interpret significant harm, how to consider sensitivity, and how to consider the number of individuals affected. A number of respondents suggested some form of matrix to allow the organization to "overlay" the incident and make a determination to report or not.

Participants requested that the OPC provide:

- an online fill-in-the-blank form or template;
- a matrix to help determine materiality;
- examples of the types of breaches the OPC would expect to be reported;
- clarity about the definitions of:
  - sensitivity;
  - commercially acceptable operating standards;
  - significant harm.
- a reporting structure that is consistent with that of provincial jurisdictions.

In addition to the specific guidance for reporting, a number of respondents also recommended that the OPC provide education for consumers to help the public understand the context of incident reporting, what organizations' responsibilities are to report, and when reporting would not be required. One responded that "customers need to know that not every breach will need to be reported and not every breach can lead to serious consequences such as identity theft."

A number of respondents also recommended that the OPC develop some training for senior executives to help them understand the purpose of reporting, how reporting will benefit the OPC, the consumer, and the organization, and what are the consequences of not reporting.

From a process point of view, several respondents asked the OPC to provide an electronic fill-in-the-blanks template to ensure that reporting is easy to execute. As one participant noted, "by creating a fill-in form, the OPC will get consistent input and save us time in trying to decide what they need to know and how much."

3.6 Reporting Anonymously to a Third Party

Respondents were given the opportunity to comment on the benefits of reporting breach incidents anonymously and to a third party, instead of directly to the OPC.

Question:

Under a mandatory regime, would the company's decision to report or not report be affected if the reporting was done anonymously and to a third party?

Eight percent (8%) of respondents preferred this reporting option, for the reason that it limited the organization's liability and exposure. Almost 60% of organizations rejected this option and stated that they would rather report directly to the OPC. As one

respondent noted, “anonymous reporting will not provide the OPC with the information needed and will undermine the whole purpose of reporting.” Of the balance (32%), most of these indicated that the decision to report or not report *may* be affected, and often stated that it might benefit others but that they would likely not prefer this option.

The only identified benefit to be derived from some sort of anonymous/third-party process would be if organizations could contact such a third party anonymously to obtain advice on whether reporting is appropriate.

4. Privacy Management Programs

In this part of the survey, organizations were asked a series of questions concerning the organization's privacy management programs. The purpose of these questions was to determine what actions, if any, organizations were taking to prepare for the implementation of mandatory reporting and the maturity of breach response and privacy management programs.

4.1 Preparing for Mandatory Reporting

Ninety-six percent (96%) of respondents reported that the organization has not taken any actions to date in preparation for mandatory reporting. As noted in Section 3.2 above, 22% indicated that mandatory breach reporting would not have any effect on their organization so it would be reasonable to expect that those organizations would not undertake any actions. The remaining organizations appear to be waiting until some further action is taken on the proposed amendment. A number of organizations stated that if mandatory reporting comes into effect they will likely be conducting further training.

Questions:

Has your company begun planning for mandatory reporting?

If so:

- What actions have been taken?
- What actions are being planned?

4.2 Breach Response Protocols

Having a formalized, documented breach response protocol is an important component of dealing effectively with privacy breaches. Fifty-two percent (52%) of organizations reported that they had such a formal, documented protocol. From these participants' responses it is clear that the structure of these protocols is mainly based on the Guidelines. These organizations stated that their policy gave them a very disciplined approach to dealing with breaches.

Questions:

Does your company have a documented, formal breach protocol in place?

If so, describe the key components.

If not, will a protocol be established to deal with the new reporting requirement?

Of the remaining 48%, more than half stated that they had an "informal" process in place, which may include, for example, using a short checklist of things the Privacy Office might ask the relevant business team to review, bringing a number of individuals together for an ad-hoc discussion as to next steps, or calling external counsel for assistance. While a number of these organizations were about to start or were in the process of developing a privacy breach protocol, not all indicated that this was something they were working on. One organization indicated that one of the reasons they did not have a policy was

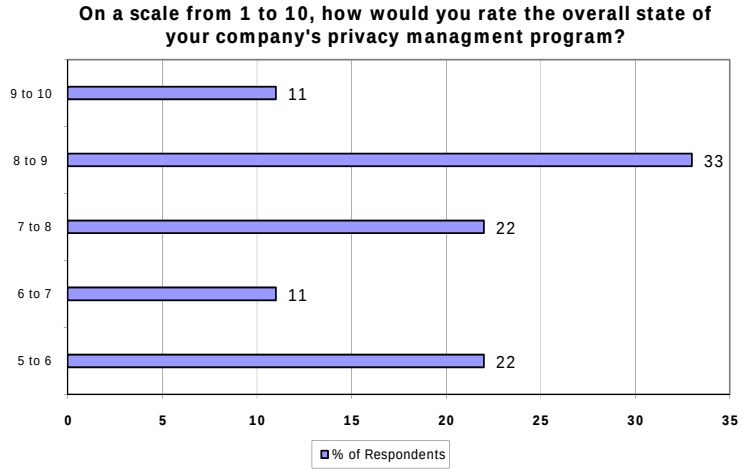
that “it did not want any other external organization interpreting what the company should or should not have done in comparison to the policy,” should a breach occur.

One-third of respondents (33%) reported the company had a formal, system-based incident tracking program in place. Typically these systems tracked all types of incidents including IT-type incidents (such as lost hardware), and incidents such as misdirected mail, inappropriate disclosures by employees, etc. The benefit of these systems is that they provided the organization with a complete overview of all incidents to allow for focused remediation efforts. One participant noted that the company “reviews privacy incidents with a privacy team every six months to determine what needs to be done,” while another respondent indicated that the information in the tracking system is “shared with the Board Audit Committee annually as part of its overall governance program.”

Fifty-two percent (52%) of respondents had some informal mechanism in place to track privacy incidents. These ranged from forms filled out by the individual responding to the breach and retained for future reference, to Excel-type spreadsheets maintained by the Privacy Office. The challenge for this type of tracking mechanism is that they tended to be anecdotal in nature and therefore a significant risk exists that not all incidents are reported.

4.3 Maturity of Privacy Management Programs

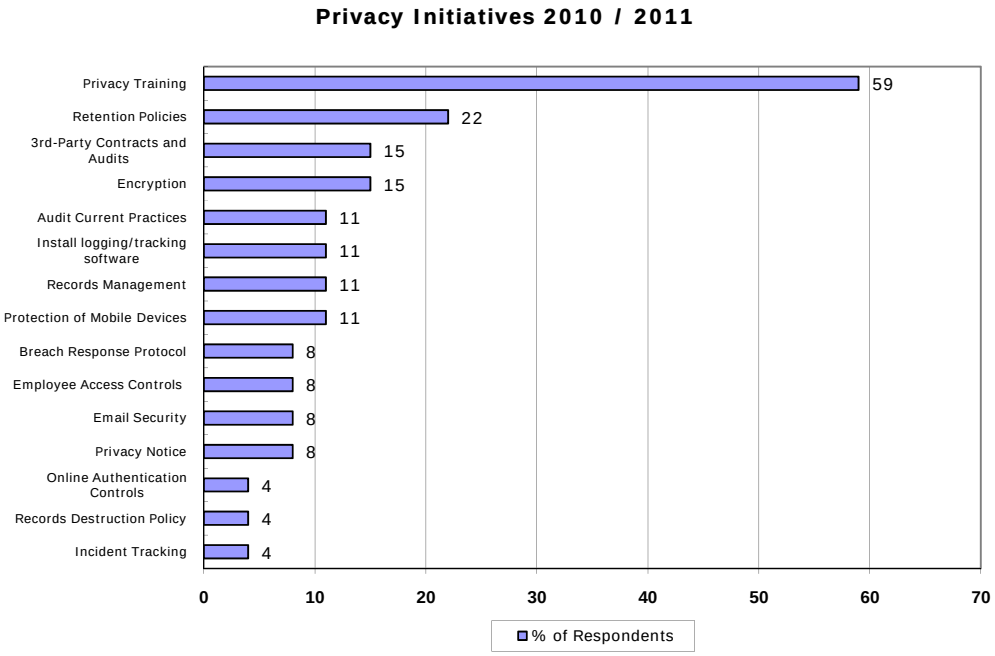
Organizations were asked to rate the overall maturity of their privacy management program on a scale from 1 to 10, with 10 being a fully mature, documented and implemented program. The following represents the participants’ ratings:



The chart clearly shows that privacy management programs are still in the development stage. A number of organizations reported the existence of an overall framework, in that they had some internal policies and privacy notices on their websites and that some training had been done. However, many recognized that they were on a privacy management journey that was ongoing. In large, decentralized organizations, and particularly those with substantial staff turnover, there was acute awareness that there was always room for improvement in both design and execution. One participant noted that "training needs to happen over and over again as every year we identify new issues and problems that we want to share with our employees."

4.4 Privacy Management Initiatives

As noted above, organizations are generally aware that privacy management requires continued updates to policies, procedures, and technical safeguards. To gain insight into what organization are doing to improve privacy management, we asked participants to identify what initiatives they were planning for the next two years. The following is a list of initiatives identified:



5. Review of OPC Breach Reporting Statistics

For a number of years, the OPC has been gathering information on private-sector privacy incidents. The OPC Investigations and Inquiries Branch provided Nymity with a summary of its findings in a report titled "Study of Incidents and Breaches: 2006–2008" (the "OPC Study").

This report provides a statistical analysis of self-reported security breaches and other privacy incidents in the private sector that occurred between January 1, 2006 and December 31, 2008 and for which OPC incident investigation files were opened.

As part of this research project, Nymity reviewed these statistics from the following perspectives:

- Do the responses of the survey align with the issues identified in the OPC Study?; and
- Are there additional data points that the OPC should collect in the future?

5.1 Survey Alignment with OPC Study

The OPC study identified the following types of incidents in order of frequency[7]:

- unauthorized access, use, or disclosure: 36%
- accidental disclosure: 31%
- theft: 24%
- loss: 10%.

While the Nymity research was not primarily focused on creating a quantitative analysis of breach statistics, the responses to our questions were relatively consistent with the findings of the OPC Study. Employees of organizations were identified as the source of most unauthorized accesses, uses, or disclosures, and as one participant noted, "the access is almost always for some malicious purpose—usually to find out information about the person that can be used against them." This was of particular concern in large organizations which hold large amounts of highly personal information, such as financial information.

Nymity's research participants also frequently referred to the types of accidental losses noted in the OPC Study, such as misdirected mail, problems with emails, and use of incorrect fax numbers.

[7] Numbers have been rounded to nearest whole number

While the OPC Study found that the lack of employee awareness/training was the second highest ranked privacy issue, a number of participants noted that in many cases the accidental disclosures, or even the inappropriate access or use incidents, were not the result of lack of training as such, but poor execution or a knowing violation of the policies. As one participant noted, “in most cases where the employee was looking at an individual’s personal information for malicious purposes, they knew exactly what they were doing, and that it was against policy.” One respondent noted that “training and awareness is not to always to tell employees something new but to reinforce something they already know.”

5.2 Additional Data Points

The OPC Study provides a thorough analysis of the source of breaches both by type and root-cause.

To support the stated purpose of providing feedback to organizations to help prevent future privacy breaches, it may be beneficial for the OPC to gather statistical and descriptive data from organizations as to the actions the organizations have taken to mitigate risks associated with the breach, and actions taken to prevent reoccurrence. While some of these measures may be proprietary in nature and may be deemed to be confidential business information in some circumstances, many of the risk mitigation strategies and tactics can be shared with other organizations. This may be particularly helpful within industry sectors, and where appropriate, the relevant industry association may be a useful partner in improving overall privacy management practices within a sector.

Appendix A. Methodology

A.1 Survey and Primer Preparation

The Survey and Primer were drafted by Nymity, and in addition to being vetted by the OPC, input on both these documents was received from privacy professionals associated with the following organizations:

- two industry associations;
- a leading privacy expert in private practice with a leading law firm;
- a telecommunications company;
- a major retailer; and
- an internet service provider.

After input was received, changes were made to both the Primer and Survey questions. A number of questions were added, modified and in some cases reordered to ensure the Survey would raise the relevant issues and discussion.

A.2 Participants:

Nymity contacted over 65 privacy professionals to solicit their input and participation, with 27 agreeing to participate.

The Primer and Survey were also made available via Nymity's website[8] to allow privacy professionals not contacted by Nymity to also participate in this research project. In addition, Nymity issued a press release announcing this study as a means of encouraging participation.

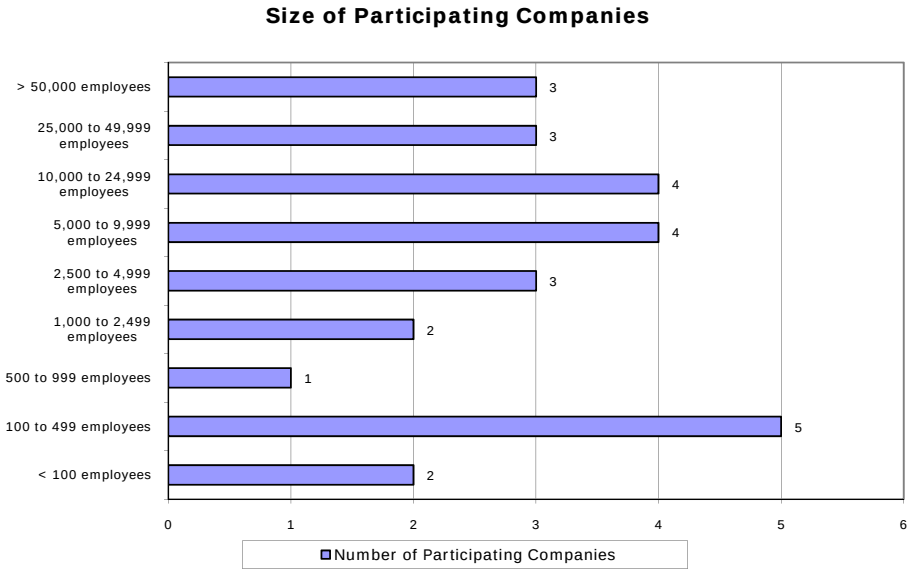
The surveys were conducted between August 27, 2009 and September 18, 2009 by means of a telephone call, which generally lasted about one hour each.

Industries surveyed included:

- Financial Services – 6 participants;
- Telecommunications – 4 participants;
- Information Technology – 3 participants;
- Insurance – 3 participants;
- Manufacturing – 3 participants;
- Retail – 3 participants; and
- Others – 5 participants.

The Survey responses were also examined considering the size of the organization, using the number of employees as a baseline measurement. The participating companies ranged in size from under 100 employees to more than 80,000 employees, as noted on the chart below:

[8] http://nymity.com/Research_Services/Research_For_Regulators.aspx


Size of Participating Companies
> 50,000 employees
25,000 to 49,999 employees
10,000 to 24,999 employees
5,000 to 9,999 employees
2,500 to 4,999 employees
1,000 to 2,499 employees
500 to 999 employees
100 to 499 employees
< 100 employees
3
3
4
4
3
2
1
5
2
0
1
2
3
4
5
6
Number of Participating Companies

Appendix B. Primer

Research Project Overview

Nymity Inc. has been engaged by the Office of the Privacy Commissioner of Canada ("OPC") to conduct a research project relating to incident reporting to the OPC.

The purpose of this research project is to gain an understanding of how organizations are currently interacting with the voluntary notification guidelines issued by the OPC. Of particular interest is the process organizations are using to determine when to notify the Commissioner's office when they have experienced a breach, for instance, what types of breaches would be reported, concerns organizations have about reporting and what incentives could be provided to encourage reporting. In addition, this research project is to gain an understanding of the impact that mandatory notification to the Commissioner would have if the proposed amendments to PIPEDA are enacted.

Participants in the survey have a unique opportunity to outline specific concerns relating to incident reporting and breach notification. Nymity will be conducting interviews with private sector privacy officers across Canada to obtain their input and feedback on the above issues. An abridged version of the interview will also be available on Nymity.com for those privacy professionals who want to participate but are not available for an interview. The study is being conducted anonymously, with no company identifying information collected during the study, included in the study report or provided to OPC. Nymity will be reporting specific feedback and trends where they exist and compiling any statistical data at industry level.

Introducing John Jager, Nymity's VP of Research Programs

The research project is being lead by John Jager, CIPP/C, Nymity's Vice President of Research Programs. John is an accredited and experienced privacy professional and has been a VP at Nymity for 3 years. His experience in privacy includes 2 years as the Chief Privacy Officer at Sears Canada Inc. John is Vice-chair of CMA's Privacy and Ethics Committee and has represented the CMA at an Industry Canada's consultation roundtable during the creation of the amendments to PIPEDA. John delivers Nymity's Breach Response Training Workshops and has created Nymity's Breach Response Centre, a component of PrivaWorks. John is conducting these interviews due to his vast knowledge of the issues related to handling privacy breaches.

Current Voluntary Reporting Guidelines

In August 2007 the OPC issued a number of documents under the title "Guidelines for Organizations in Responding to Privacy Breaches". The guidelines included key steps for organizations to take when responding to privacy breaches and also included a privacy breach checklist.

In the document "Key Steps for Organizations in Responding to Privacy Breaches" section 3 deals with the matter of notification. This section provides guidance as to whom, how and when relevant parties should be notified when a breach occurs. Section 3(iv) - Others to Contact discusses reporting the breach to parties other than those directly affected by the breach.

The OPC encourages organizations to report material privacy breaches to the appropriate privacy commissioner(s) as this will help them respond to inquiries made by the public and any complaints they may receive. In addition, the OPC may be able to provide advice or guidance that may be helpful in responding to the breach.

When considering providing notification to the OPC the following factors should be considered:

- any applicable legislation that may require notification;
- whether the personal information is subject to privacy legislation;
- the type of the personal information affected;
- whether the disclosed information could be used to commit identity theft;
- whether there is a reasonable chance of harm from the disclosure, including non-monetary losses;
- the number of people affected by the breach;
- whether the individuals affected have been notified; and
- if there is a reasonable expectation that the privacy commissioner's office may receive complaints or inquiries about the breach.

It is important to note that currently there is no statutory requirement in PIPEDA (or in the Alberta and B.C *Personal Information Protection Act*) to provide notification of breaches to either affected parties or any other party, but that to do so is encouraged by the privacy commissioners across Canada.

Proposed Amendments to the Personal Information Protection and Electronic Documents Act (PIPEDA)

During 2006 and 2007 the House of Commons Standing Committee on Access to Information, Privacy and Ethics (the "Committee") undertook a

statutory review of PIPEDA as required by the Act. The Committee issued its recommendations in a report in May 2007.

Recommendation 23 of the Committee's report recommended that "PIPEDA be amended to include a breach notification provision requiring organizations to report certain defined breaches of their personal information holdings to the Privacy Commissioner".

Industry Canada subsequently held a number of meetings with interested stakeholders to develop a proposed framework that could form a basis for amendments to PIPEDA. In its June 2008 report Industry Canada published a working model to assist in framing and considering proposed legislative amendments to PIPEDA.

Part B - Section 3 of the Industry Canada report deals with the requirement to report to the Privacy Commissioner of Canada and recommends that the requirement for reporting be defined along the following lines:

> "An organization will be required to report to the Privacy Commissioner any material data breach. Factors relevant to the determination of a material data breach are (i) the sensitivity of the information involved in the breach, (ii) the number of individuals affected, and (iii) whether the data breach constitutes a pattern, or provides evidence of a systemic root-cause outside of commercially acceptable operating standards."

In determining who is to notify the Privacy Commissioner the report recommends that the organization having control of the information will be responsible for determining the need for reporting a data breach. This recommendation is meant to deal with issues such as breach of personal information in the possession of third-party service providers.

The report recommends that the Commissioner be notified as soon as reasonably possible following detection, confirmation and an assessment of the scope and extent of the breach. The report also outlines some of the relevant information that should be contained in a report to the Commissioner including such as:

- organization name and industry sector;
- circumstances of the data breach;
- types of information involved;
- what notification has been undertaken or is planned; and
- steps taken to contain the breach.

As of writing the government has not introduced any legislative changes to PIPEDA that includes this framework for reporting to the Privacy Commissioner, but it is generally expected that activity on this front is expected during the legislative session commencing fall 2009.

Key Terms and Definitions

"Personal Information":

- information about an identifiable individual, but does not include the name, title or business address or telephone number of an employee of an organization (PIPEDA Section 2(1).

"Privacy Breach":

- an unauthorized access to or collection, use, or disclosure of personal information:
    - activity is "unauthorized" if it occurs in contravention of applicable privacy legislation.

  (as defined in the "Key Steps for Organizations in Responding to Privacy Breaches" issued by the OPC)

"Material Breach":

- factors relevant to the determination of a material breach include:
    - the sensitivity of the information involved in the breach;
    - the number of individuals affected; and
    - whether the breach constitutes a pattern, or provides evidence of a systemic root-cause outside of commercially acceptable operating standards.

The Research Survey

The survey will be conducted by phone and consists of a number of questions that are crafted to solicit qualitative answers. The research study will collect some quantitative information. Please be assured that all this data is collected anonymously, and in no way will any information provided in confidence in this survey be used or disclosed. All statistical data will be recorded and tracked separately from the balance of the survey to more fully ensure the information cannot be linked any particular organization.

To assist participants in collecting the data prior to the phone survey, the questions that require a quantitative answer for statistical purposes are included below:

Question 1 – Estimate the number of incidents reported to the organizations Privacy Office/Privacy Officer:

- in 2008
- anticipated after mandatory reporting comes into effect

Question 2 - Estimate the number breaches of PI in 2008 by severity level as deemed by the company:

- Severe
- Moderate
- Mild

Question 3 - Estimate the number of breaches of customer or employee personal information:

- Customer PI
- Employee PI

Question 4 - Estimate the number of breaches reported to the OPC:

- in 2008
- anticipated after mandatory reporting

APPENDIX C. Survey

Section 1 – Company information:

- Industry:
- Company Size - approx # of employees

Section 2 – Current Voluntary Reporting Regime:

As outlined in the primer, the Office of the Privacy Commissioner has issued a guideline titled Key Steps for Organizations in Responding to Privacy Breaches. Organizations are encouraged to report material privacy breaches to the appropriate privacy commissioner(s) considering a number of factors such as applicable legislation, type of personal information (PI) affected, number of individuals affected and if affected parties have been notified. This section of the interview seeks information relating the current voluntary reporting regime.

Question 1: Are you/your organization aware of the currently voluntary breach notification guidelines and how they apply to you?
Question 2: In the past has your organization experienced any incidents where data was lost?
Question 3: What processes/procedures does your company have in place to help it identify and assess that a potential breach or data loss has occurred?
Question 4: When it is determined that a breach of PI has occurred how is the decision to notify the OPC made?
Question 5: In what circumstances would the OPC be notified?
Question 6: Has the organization experienced a data loss incident where there was a risk of significant harm to the affected parties, and a decision was taken not to notify the OPC? Can you explain why the OPC was not notified?
Question 7: What are the opinions of senior management regarding voluntary breach reporting to the OPC? What are their concerns about reporting or not reporting?
Question 8: What actions or incentives can the OPC put in place to encourage reporting of breaches?
Question 9: What support processes can be provided by the OPC that will facilitate voluntary reporting to the OPC?
Question 10: Have you had any breaches of PI of Canadians that have taken place outside of Canada? If yes: what actions were taken by the organization in response to the breach? If not: is there a policy in place that deals with this situation? What is included in this policy?
Question 11:

Have you had any breaches of PI relating to PI that was shared with a third-party? If so: was there a protocol in place to deal with this breach? If not: is there a policy in place to deal with these types of breaches? What is included in this policy?
Question 12: If a breach has been reported to the OPC how would you describe the overall experience?
Question 13: Would you describe your organization as having an open and honest culture of reporting incidents of data loss?
Question 14: What do you believe is the reason and purpose that the OPC is requesting organizations to voluntarily report breaches?

Section 3 –Mandatory Reporting Regime:

As outlined in the primer, Industry Canada will be recommending that the amendments to PIPEDA include a mandatory reporting regime requiring organizations to report to the Privacy Commissioner any material data breach. This section seeks to explore challenges organizations may face in a mandatory reporting regime.

Question 1: Based on the information in the primer regarding the proposed amendments, has your organization experienced any data loss incidents in the past that were not reported to the OPC that would now be reportable? If so – what are the factors that would have made those incidents reportable under a mandatory regime?
Question 2: Are there any new concerns created by the mandatory reporting of breaches to the OPC and why?
Question 3: Under a mandatory reporting regime would the process to decide on when to report be different than it is today?
Question 4: Under a mandatory reporting regime would a company's decision to report or not report be affected if the reporting was done anonymously to a third-party?
Question 5: What factors might reduce any hesitancy to report?
Question 6: If/when reporting becomes mandatory what support do you need to assist you in helping conform to the new requirements?

Section 4 – Potential Impact of Mandatory Reporting on Organizations

This section includes a number of questions that explores the potential impact that the proposed mandatory reporting may have on organizations. The impacts could include those of a financial nature, the need to update privacy management protocols or even structural changes in how organizations execute their privacy programs.

Question 1: What impact do you believe that mandatory reporting will have on your company?
Question 2: Has your company already begun planning for mandatory reporting? If so: what actions have been taken? what actions are being planned?
Question 3: Does your company have a formal breach protocol in place? If so: describe the key components of the protocol ; If not: will a protocol be established to deal with the new reporting requirements?
Question 4: Does your company have an incident tracking program in place? If so: describe the key components of the program; If not: will an incident tracking program be established to deal with the new reporting requirements?
Question 5: How would you describe the overall state of your company's privacy management program?
Question 6: In addition to the issues relating to mandatory reporting is your company investing any additional resources to improve/support the privacy management program in 2010? in 2011? If so, describe the types of investment being considered?

Section 5 – Quantitative Measures:

This section will collect from participants available data regarding incidents and/or breaches that have occurred within the organizations. Please note that any data collected is done so anonymously and is meant for summarization and general trending purposes.

If available please provide the following data:

Question 1: Estimate the number of incidents reported to the Privacy Office/Privacy Officer: • in 2008: • anticipated after mandatory reporting:
Question 2: Estimate the number breaches of PI in 2008 by severity level as deemed by the company: • Severe: • Moderate: • Mild:

Question 3: Estimate the number of breaches of customer or employee personal information**:** • Customer PI: • Employee PI:
Question 4: Estimate the number of breaches reported to the OPC: • in 2008: • anticipated after mandatory reporting:

APPENDIX D. Letter from Terry McQuay, President, Nymity Inc.

To: Readers of the OPC Incident Reporting Research report

From: Terry McQuay, President, Nymity Inc.

Re: Comparison of survey results with Nymity's interaction with privacy professionals

As this research project was conducted independently by John Jager, Nymity's VP of Research Programs, I was not directly involved in the research study or the creation of this report. Therefore, I was very curious to read the outcome of this research study to see if the results were reflective of my personal experience when working with corporate Canada. Nymity's business model includes a direct outreach program through which we contact Privacy Officers at companies of all sizes to introduce our offerings. The outreach program is not selective, but contacts organizations randomly without knowledge of how seriously they take privacy and how proactive they invest in privacy management and compliance. I personally speak with over 150 Privacy Officers per year and my experience has been that:

1. Organizations are aware of privacy law and while not all organizations have someone with the title of Privacy Officer, there is someone responsible for privacy. Typically, it is easy to find the individual responsible for privacy – we contact the company, ask for the legal department and then ask that individual who responsible for privacy. In smaller organizations, often there is not a legal department but they always know who to call for legal issues;
2. Organizations that collect any customer personal information have a privacy policy;
3. Most organizations that collect customer personal information have conducted some form of employee training;
4. Most organizations with sensitive information have gone beyond policies and training and have:
    a. procedures in place and in some cases have created detailed privacy handbook;
    b. created a breach protocol.
5. Most organizations have not had many complaints, if any, and few access requests;
6. Organizations with a head office in British Columbia and Alberta generally have a more mature privacy management program then elsewhere in Canada, and these organizations have done more in the area of employee privacy. In Alberta, we have seen small businesses with very mature privacy management programs.

For the most part my observations and experiences in dealing with privacy professionals across Canada are consistent with these study results and I am not surprised by the level of awareness that organizations have related to the Commissioner's guidelines for breaches. I had expected that organizations would be more concerned about self-reporting breach incidents to the OPC and those organizations would have preferred to report incidents

anonymously. The high level of trust when working with the Commissioner's office is very likely due to reputation the OPC has built with the privacy community over the last four years.

I believe organizations' investment in privacy management are related to the following factors:

1. The sensitively and amount of information collected;
2. If the organization's head office is in British Columbia or Alberta;
3. Corporate culture;
4. Age of the organization; and
5. Personal beliefs of the Privacy Officer.

Based on my extensive dealings with Privacy Officers across Canada, I believe this study is representative of corporate Canada. I am confident that the process used for the study was meticulous followed to ensure the collection of accurate and representative content.

About Nymity

Nymity is a global privacy and data protection research services firm specializing in compliance and operational risk management, known best for its world leading research tool, PrivaWorks, used by over 1,000 privacy professionals. Nymity created the PbD Risk Optimization Methodology

recognized as an excellent privacy management tool for implementing privacy and data protection into business activities. Nymity has made the methodology available to privacy community. Nymity's research spans across the United States, Europe and Canada and will include the Asia-Pacific Rim and South America in 2010.