Office of the
Information & Privacy
Commissioner
for British Columbia

Protecting privacy. Promoting transparency.

AN EXAMINATION OF BC GOVERNMENT'S PRIVACY BREACH MANAGEMENT

Elizabeth Denham
Information and Privacy Commissioner

January 28, 2015

CanLII Cite: 2015 BCIPC No. 65
Quicklaw Cite: [2015] B.C.I.P.C.D. No. 65

TABLE OF CONTENTS

COMMISSIONER'S MESSAGE

Public awareness and concern about privacy breaches is on the rise. New technology and the growing use of electronic records have made privacy breaches more prevalent, affecting citizens in greater numbers.

It seems not a week goes by without a high-profile media story about hackers exploiting security vulnerabilities in card payment systems, lost or stolen laptops, unencrypted USBs, or employees "snooping" at personal records.

The tangible impact of a privacy breach can be physical or economic. Breaches can also create profound intangible harms such as embarrassment, anxiety, discrimination, and a sense of intrusion into one's private life. Privacy breaches can also lead to social harms such as a loss of public trust in the use of electronic records or government institutions as a whole.

This special report, the first in my Office's new Audit & Compliance Program, examines the degree to which government is fulfilling its duty to respond to, and properly manage, its privacy breaches.

I have chosen to focus on core government because public institutions occupy a trusted position in the lives of citizens. Individuals often have no choice but to hand over their personal information in exchange for the services such as health care, education or other social benefits. This privileged position of trust leads to a heightened expectation that government will have appropriate safeguards in place to protect personal information.

Given the volume and sensitivity of personal information government collects from millions of British Columbians, my expectation going into this examination was that government would be setting the bar high for the detection, resolution, and prevention of privacy breaches.

This report makes several important recommendations that, if adopted, will help government enhance the efficacy of its breach management programming and build trust among citizens. I also hope that other public bodies find this information useful in the implementation of their own privacy programs.

At the conclusion of this examination, I am carefully considering whether to recommend that the *Freedom of Information and Protection of Privacy Act* needs a legislated requirement to notify individuals and my Office when significant privacy breaches occur. I made a similar recommendation to the BC Legislature in 2014 for the *Personal Information Protection Act*, BC's private sector legislation.

I intend to study this issue further as my Office expands its examination of breach management to other public bodies in BC. In the meantime, this report establishes an interim standard for reporting privacy breaches to my Office. I expect government to follow this standard going forward.

I will be following up with government in three months' time to gauge implementation of all of the recommendations.

January 28, 2015

ORIGINAL SIGNED BY

Elizabeth Denham
Information and Privacy Commissioner
for British Columbia

EXECUTIVE SUMMARY

A privacy breach occurs when there is unauthorized access to or collection, use, disclosure or disposal of personal information. Such activity is "unauthorized" in the British Columbia context, if it occurs in contravention of the *Personal Information Protection Act* ("PIPA") or Part 3 of the *Freedom of Information and Protection of Privacy Act* ("FIPPA").

Since there will never be 100% assurance that one's personal information will not be treated in an unauthorized fashion, the management of privacy breaches is an important responsibility of both private sector organizations and public bodies.

Citizens are looking for assurance that local and provincial government bodies are protecting their personal information and expect the Office of the Information and Privacy Commissioner ("OIPC"), as the oversight body, to gauge the level of compliance with safeguarding requirements and to assist public bodies in achieving accountable privacy management programs. As such, the OIPC decided to conduct a comprehensive review of the British Columbia Government's breach management practices.

Under the authority of section 42(1) of FIPPA*,* the OIPC conducted an examination of the efficacy of the management of privacy breaches within the Government of British Columbia. The key objectives of this examination were to review the extent of compliance with relevant legislation, policies and procedures and, where appropriate, to make recommendations to strengthen such legislation, policies and procedures.

The examination included:

- a review of FIPPA and the Office of the Chief Information Officer ("OCIO") policies and procedures relating to privacy breach management;
- interviews with OCIO privacy breach investigative staff and branch management;
- an inspection of OCIO investigative files;
- a review of select ministry-specific policies and procedures relating to privacy and breach response; and
- interviews with key information and security staff within select ministries.

The examination revealed that government has a solid foundation in place for managing privacy breaches and that the majority of suspected breaches are reported to the OCIO within a day or two of discovering the incident, are contained, and are investigated within a reasonable timeframe. Ministries provided notifications to affected individuals when appropriate, and written notifications included all of the necessary information. The OCIO also provided advice on preventative measures in almost every investigation.

There are, however, opportunities for improvement as gaps were found in relation to audits of security safeguards, analysis and public reporting of breaches, follow-up on implementation of preventative measures, timeliness of notifying individuals who may be impacted by a breach, internal processes for documenting and tracking breaches, and training participation rates.

There is also a lack of clarity around when breaches should be reported to the Information and Privacy Commissioner.

In order to address these gaps and achieve an accountable privacy management program, the government needs to build on the solid foundation it has established. Government should take advantage of the centralized repository for information about breaches that it has created within the OCIO and utilize the available information to achieve long term solutions for protecting personal information. Correspondingly, the OIPC recommends that the government establish an ongoing privacy compliance monitoring function within the OCIO.

The OCIO is in a unique position to provide cross-government monitoring of privacy management functions by conducting audits of privacy safeguards and analyzing trends in privacy breaches. Privacy compliance monitoring would allow the OCIO, and thereby the government, to analyze the root causes of privacy breaches, mitigate harms, identify solutions to reduce the risk of future breaches, and become a trusted advisor to ministries by providing information and expertise regarding how best to safeguard the personal information they collect and use.

In addition, providing a privacy compliance monitoring function and producing public reports can instill citizens with the confidence that the government protects their personal information. It cannot be overstated how important ongoing privacy compliance monitoring is to an effective and accountable privacy management program.

The public also expects effective oversight of the government's collection, use and safeguarding of personal information. Open, accountable and transparent communication with the OIPC, particularly with regard to reporting breaches that occur, is key to the oversight function and is in the public interest.

This examination has found that privacy risk evaluation processes lack clarity and that there are no specific standards that delineate when public bodies need to report suspected breaches to the OIPC, nor when to notify individuals affected by a privacy breach. The OIPC recommends that, as an interim measure, the government report all suspected breaches to the OIPC if the suspected breach involves personal information, and could reasonably be expected to cause harm to the individual and/or involves a large number of individuals.

In addition, this examination found opportunities for the OCIO to improve internal procedures for documenting and categorizing privacy breaches that will assist in effectively assessing risk of harm in individual breaches, determining when to provide notifications to affected individuals and to the OIPC, identifying systemic issues to mitigate reoccurrence, and providing centralized governance of the government's breach management process.

Finally, this examination also pointed to the need for increased participation in training relating to the importance of protecting personal information, breach management processes and the OCIO's role. This training would assist in ensuring that government employees are aware of their obligation to protect personal information, breaches are managed properly when they do occur, notifications to affected individuals occur without unnecessary delay, and breaches are reported to the OIPC.

1.0 INTRODUCTION

The Office of the Information and Privacy Commissioner for BC ("OIPC") provides independent oversight and enforcement of British Columbia's *Freedom of Information and Protection of Privacy Act* ("FIPPA") and the *Personal Information Protection Act* ("PIPA") and related regulations.

The OIPC's Audit & Compliance Program involves evaluating the extent to which public bodies and private sector organizations are protecting personal information and complying with FIPPA, PIPA and related regulations.

This first assessment within the Audit & Compliance Program examines the efficacy of the management of privacy breaches within the Government of British Columbia. Conducted under the authority of s. 42(1) of FIPPA, this assessment is intended to form part of a larger review of privacy breach management processes across the broader public sector.

Effective breach management is important to the citizens of British Columbia. Public bodies collect sensitive personal information in order to administer many of their programs. Members of the public are concerned about the protection of their privacy and need assurances that they can trust public bodies to appropriately safeguard their personal information and if it is released in an unauthorized fashion, that appropriate follow up steps are taken. An essential part of building and maintaining public confidence is responding appropriately whenever personal information has been compromised, which includes notifications of affected individuals and reporting to the appropriate oversight authority. Such accountability and transparency are key aspects of effective privacy breach management.

There has been an upward trend in the number of breaches within government; however, there has not been a corresponding increase in the reporting of breaches to the OIPC by government. This is not necessarily a problem, however, it is concerning that only a small number of privacy breaches are reported to the OIPC by public bodies in general, and in particular, by those that collect large amounts of sensitive personal information. Recognizing that British Columbia does not currently have mandatory breach reporting requirements, if the OIPC is not informed about breaches, it cannot provide oversight to ensure that public bodies are meeting their obligations with respect to safeguarding personal information and effectively managing privacy breaches.

Citizens expect the OIPC, as the oversight body, to gauge the level of compliance with safeguarding requirements and to assist public bodies in achieving effective privacy management programs. As such, the OIPC decided to conduct a comprehensive review of the government's breach management practices.

The objectives of this examination are to:

- examine the legislation, policies and procedures relating to the management of and response to privacy breaches;
- review the extent of compliance with the legislation, policies and procedures;
- identify the main trends and key risk factors involved in privacy breaches; and
- where appropriate, make recommendations to strengthen policy, practice or legislation.

The scope of the examination included:

- **OCIO Process Review**: A review of relevant Office of the Chief Information Officer ("OCIO") policies and procedures. This included an overview of the mandate of the OCIO, interviews with staff and management, analysis of the policies and procedures that define how information incidents and privacy breaches are to be managed, developing an understanding of the government's privacy breach investigative process, and an overview of the mandatory privacy training provided to government staff.

- **File Review**: An inspection of OCIO investigative files and other relevant information based on: the OIPC's recommended steps for responding to privacy breaches (containment, risk evaluation, notification, and prevention strategies), the responsibilities set out in FIPPA and relevant government policies and procedures.

- **Ministry Processes Review:** A review of ministry-specific policies and procedures relating to privacy within select ministries where breaches have occurred. This also included interviews with key information and security staff from four key government ministries: Social Development and Social Innovation ("SDSI"), Children and Family Development ("MCFD"), Health ("MoH") and Justice ("JAG").

See Appendix A for more detail regarding the methodology used for this examination.

The purpose of this report is to document, describe, comment and recommend improvements regarding the government's management of privacy breaches, taking into consideration public bodies' obligations under FIPPA. The report outlines legislative and policy directives, presents findings from the examination and, in a separate section, discusses key issues and recommendations to address those issues.

2.0 APPLICATION OF SECTION 30 OF FIPPA

A privacy breach involves the unauthorized access to or collection, use, disclosure or disposal of personal information.[1] Privacy breaches can be unintentional or deliberate and may range anywhere from government mail containing personal information being delivered to the wrong individual, to unauthorized access to databases of personal information by government employees, to disclosure of personal information of confidential informants in child protection or criminal investigations.

Managing privacy breaches forms part of the duty to protect personal information.[2] Section 30 of FIPPA governs privacy breach management and establishes a public body's obligation to protect personal information. Section 30 of FIPPA states:

> A public body must protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal.

OIPC investigation reports and guidance documents have noted that a public body cannot meet the requirements of making reasonable security arrangements without including measures to ensure appropriate and effective management of privacy breaches, determining whether affected individuals should be notified, and considering whether to report breaches to the OIPC. For example:

- Investigation Report F06-02 concluded that the s. 30 reasonable security standard includes developing appropriate policies and procedures relating to personal information protection, including protocols for dealing with privacy breaches.[3]
- Investigation Report F13-02 states that a public body's obligations under s. 30 include the actions it takes when there has been a privacy breach.[4]
- In Investigation Report F06-02, the OIPC determined that reasonable security measures contemplated in s. 30 of FIPPA may require a public body to notify affected individuals of a privacy breach.[5]
- In Investigation Report F08-02, an inappropriate delay of notification of affected individuals was considered to be a failure by the public body to meet its s. 30 obligations.[6]
- The OIPC's *Accountable Privacy Management in BC's Public Sector* and *Privacy Breaches: Tools and Resources* state that the OIPC expects public bodies to promptly notify affected individuals and to report privacy breaches to the OIPC where appropriate.[7]

FIPPA itself does not currently contain specific language with respect to reporting breaches, either to affected individuals or to the OIPC. However in order for a public body to meet its obligations under s. 30 of FIPPA, it must include consideration of these steps as part of effective and appropriate privacy breach management.

3.0 OVERVIEW OF PRIVACY BREACH MANAGEMENT IN BC GOVERNMENT

Under FIPPA, individual ministries are independent public bodies[8] and are, therefore, individually responsible for complying with s. 30. Ministries are ultimately responsible for dealing with privacy breaches, notifying affected individuals and reporting breaches to the OIPC.

In May 2006, Cabinet mandated that the Chief Information Officer ("CIO") have governance authority for standards setting, oversight and approvals for the province's information and communications technology.[9] This authority is outlined in Chapter 12 of the government's *Core Policy and Procedures Manual* ("Core Policy").

The OCIO is also responsible for the *Document Disposal Act*, the *Electronic Transactions Act*, FIPPA and PIPA and "all policy standards and directives that flow from them".[10] The OCIO develops, proposes and maintains government-wide information management (information technology management) policy, procedures and standards and evaluates compliance, including in the areas of information management, privacy and security.[11]

In October 2009, at the direction of the Minister of Citizens' Services, the OCIO undertook an internal review of a privacy breach involving the Ministry of Housing and Social Development and the Ministry of Children and Family Development. The internal review resulted in a number of recommendations, one of which was to "establish a central authority within the [OCIO] with overall responsibility for managing information incidents including policy, audit, investigations and police liaison".[12]

In 2010, the British Columbia government instituted a centralized information incident management process, including a policy requiring privacy breach reporting to the OCIO.[13] The OCIO's Privacy and Legislation Branch ("Branch") provides corporate privacy services such as the development of policy with respect to the management of breaches and the development and delivery of training. It also provides guidance to ministries on the development of privacy impact assessments, research agreements and information sharing agreements, develops privacy protection schedules for contracts and publishes the Personal Information Directory.[14] The Branch's Privacy Investigations Unit ("PIU")[15] is responsible for investigating privacy complaints and manages privacy breaches on behalf of government.

3.1 BC Government Information Incident Management Process

The government's centralization of the information incident management process within the OCIO does not mean that individual ministries have transferred their FIPPA responsibilities to the OCIO. Rather, as articulated in Investigation Report F13-02, it means that it is necessary for the OCIO and the ministries to develop policies that clearly delineate which party is responsible for each aspect of a privacy management program.[16]

According to the Core Policy and the *Information Incident Management Process* ("IIMP"),[17] information incidents (relating to all information security issues, not just breaches of personal information) must be reported to the OCIO. The IIMP, developed in 2011, "defines the steps that must occur in response to an information incident, including the roles and responsibilities of the stakeholders". The IIMP is a detailed document regarding government's process for reporting an information incident. It defines information incidents as follows:

> An **information incident** is a single or a series of unwanted or unexpected events that threaten privacy or information security. Information incidents include the collection, use, disclosure, access, disposal, or storage of information, whether accidental or deliberate, that is not authorized by the business owner of that information.[18]

The IIMP outlines a thirteen step process regarding information incidents. Steps one and two require immediate reporting to one's supervisor or designated management contact and to the OCIO. The PIU does not track compliance with this policy.

It is important to note that all privacy breaches constitute information incidents but not all information incidents are privacy breaches. The IIMP states the following with respect to privacy breaches:

> Information incidents include **privacy breaches**, which are a collection, use, disclosure, access, disposal, or storage of **personal** information, whether accidental or deliberate, that is not authorized by the *Freedom of Information and Protection of Privacy Act*….[19]

The IIMP states that "privacy breaches are resolved in accordance with government's *Process for Responding to Privacy Breaches".*[20]

3.2 BC Government Process for Responding to Privacy Breaches

The government's *Process for Responding to Privacy Breaches* policy sets out the steps that ministries must follow when responding to a privacy breach. It also states that the OCIO is responsible for the coordination, investigation and resolution of information incidents, and that all actual or suspected information incidents must be reported immediately to one's supervisor and to the OCIO.

The policy requires immediate remedial action on all known or suspected privacy breaches, regardless of the sensitivity of the personal information. The policy also points out that the nature of the response depends on the circumstances of each case. The process steps for responding to a privacy breach include: immediate reporting, breach containment, assessment of the extent and impact of the privacy breach, documentation of the privacy breach and corrective action taken, consideration of notification of affected individuals, informing other parties as appropriate, and prevention of future privacy breaches.

3.3 Ministry-specific Policies and Procedures

According to ministry information and security staff, while all of the ministries follow the OCIO and core policies and procedures related to the handling of privacy incidents, each of the four ministries reviewed have additional requirements for managing breaches.

Social Development and Social Innovation ("SDSI")

In addition to requiring staff to report information incidents to the OCIO, SDSI has a parallel ministry process that includes an SDSI-specific Information Incident Checklist that must be worked through. This checklist essentially walks an individual through the various steps of reporting to the OCIO and certain ministry staff, working with the OCIO during the investigation of the breach, detailing procedures for notifications to affected individuals, and closing of internal files after the OCIO process has been completed.

A corresponding ministry-specific policy (the Information Incident Response Process) was developed for the SDSI Information Security Team and details the triggers, service levels and process steps team members perform during a breach investigation, along with the information incident contacts from within the ministry who must be informed when a breach occurs. SDSI has also documented process steps for staff in how to prevent administrative errors and has developed guidelines for service providers.[21] SDSI makes the above information available to all staff on the SDSI intranet, produces regular newsletters on its information security intranet website and holds meetings for staff to discuss privacy and related issues.

Ministry of Children and Family Development ("MCFD")

MCFD indicated that it follows OCIO and Core policies and procedures for privacy incidents. It also has posted breach reporting procedures, along with a directive requiring all staff to report all real or suspected privacy and security breaches to the OCIO, on its intranet site. When a privacy breach occurs, MCFD identifies a ministry representative who works with the OCIO investigator in managing the breach. MCFD also relies on field staff to determine risks and whether to notify. MCFD processes for responding to breaches are described as follows:

> During each investigation our first priority is to work with PIU and field staff to determine risk of harm to individual(s) or government; field staff are heavily relied upon to determine harms to individual(s) as they have the knowledge and client relationship needed to make that assessment. Once the risk of harm has been mitigated we move to containment then determine if notification is required, and finally at the closing of the incident we work to determine what prevention measures could prevent future incidents of similar nature.[22]

MCFD has a number of its own prevention processes and awareness activities, over and above the government mandated privacy training, including program-specific training and program-specific policies related to privacy and information sharing.[23]

Contracts with MCFD service providers contain requirements for the protection of personal information and the notification of the BC Government in the event of a breach (in accordance with the general services agreement).[24] MCFD has also produced guidelines to assist service providers in achieving best practices in relation to information management.[25] These *Contractor's Records Guidelines* are intended to ensure contractors understand "obligations to ensure proper information management practices are implemented and maintained".[26] Any breach reported by a contractor is to be reported to and investigated by the OCIO.

Ministry of Health ("MoH")

Separate from core government, the MoH has an *Information Privacy Policy*, the purpose of which is to establish the guiding principles and framework by which the MoH and its staff comply with their value-based, ethical and legal obligations relating to personal information in their custody or under their control.[27] This policy states that staff must report any actual or suspected privacy breaches in accordance with the process set out in the OCIO's IIMP.[28] MoH reports incidents to the OCIO and works with the OCIO to resolve the matter.

Ministry of Justice ("JAG")

JAG has a number of branches (for example, Court Services Branch, Criminal Justice Branch and Corrections Branch) that each have supplemental processes for managing information incidents.

Criminal Justice Branch's process reportedly includes assessing the nature of a breach on the basis of physical safety risk to individuals and the impact to the prosecution file. It also provides general information with respect to incident/privacy breach reporting requirements and the containment of the breach and recovery of the information.[29]

Corrections Branch's *Management Service Policy Manual* contains a chapter on information incidents that "guides how staff manage information incidents in a way that is consistent with policy established by the [OCIO]". [30] Corrections Branch's policy also included additional internal reporting steps that, at the time of reporting, were undergoing revision.

Information provided by Court Services Branch details supplemental critical incident reporting processes for sheriffs and occurrence reporting processes for court administration staff. Accordingly, when an information incident occurs, the OCIO's IIMP is reportedly also triggered in addition to these separate processes.

The existence of specific ministry policies in addition to the broader cross-government breach management policies like the IIMP and *Process for Responding to Privacy Breaches* can be a step toward effective privacy governance. In OIPC Investigation Report F13-02, the Commissioner noted that:

> A key component of good privacy governance is a clear accountability policy that designates who is responsible for the various aspects of the privacy management program. Greater clarity about the respective roles and responsibilities of the Minister, the OCIO, the MCIOs, and other branches of the Ministry helps all employees to do their part in ensuring effective privacy management.[31]

Review of the IIMP, the *Process for Responding to Privacy Breaches,* and the specific ministry policies has shown that there is some overlap between the processes prescribed in the various policy documents. It is not immediately clear within the documents how the various policies are to interact with one another.

3.4 Privacy Investigations Unit ("PIU") Process

PIU management[32] noted that the intention of the OCIO's privacy breach management process is to ensure that when a breach occurs it is quickly contained, thoroughly investigated and appropriately resolved. PIU management and staff noted that PIU investigators receive training through a combination of four one-hour training sessions, bi-weekly discussions/file reviews, instructional emails, and one-on-one training and support.

PIU management and staff stated that the OCIO breach investigations include reporting breaches, recovering the information, providing an appropriate remedy and preventing further breaches.

The IIMP describes an information incident investigation as including working with the affected ministry so the ministry can notify affected parties, take other required actions as appropriate, and provide status reports to the PIU and the Ministry Chief Information Officer.[33]

According to the IIMP, the PIU takes the lead for privacy breaches and the PIU Director provides status reports of major incidents to the CIO.[34] Where necessary, the CIO may liaise with the responsible ministry's executive and the OIPC. In some cases, a final report may be prepared which can include "mandatory" recommendations (directives) or "advisory" recommendations.[35]

While there is no legislated mandate for the OCIO to enforce compliance with its recommendations, the IIMP states that "mandatory" recommendations must be implemented, and the responsible ministry decides on implementation of "advisory" recommendations. Policy dictates that compliance with the implementation of "mandatory" recommendations falls to government, the ministry or the business owner as applicable and their status and results must be reported to the Ministry Chief Information Officer, the Chief Information Security Officer and the Director of the PIU for incidents involving personal information.[36]

3.5 Mandatory Privacy Training

Another recommendation resulting from the OCIO's October 2009 internal review was to "enhance education and training to ensure all employees are aware of information privacy management obligations and practices".[37]

In 2011, the British Columbia government instituted mandatory privacy training for all government employees.[38] The BC Public Service Agency provides an online course entitled "IM 111: Information Sharing and Privacy Awareness Training for Employees" for all government employees along with "IM500 and IM550—Executive Role in Information Sharing" for executives.

While it was outside the scope of this examination to review the content of privacy training curriculum, the abstract for the employee course notes that the curriculum is intended to provide training:

> Focussing on the employee's role and responsibilities in handling personal and confidential information and preventing information incidents in the workplace. Participants will learn how to handle information incidents, including privacy breaches.[39]
>
> The purpose of the course is to:
>
> - build understanding and support a culture of privacy awareness of responsible information sharing; and
> - develop capacity to respond effectively and correctly when breaches and information incidents (including privacy breaches) occur.
>
> Upon completion, [participants] will be able to:
>
> - support a culture of responsible information sharing and compliance with privacy legislation and government policy;
> - be aware of information sharing, privacy policy and processes;
> - understand your role and responsibilities in information sharing and privacy; and
> - identify when an information incident, including a privacy breach, has occurred and know what actions to take.[40]

PIU management reported that they believe mandatory privacy training for government employees has resulted in increased awareness of breach reporting requirements, knowledge of the PIU and reporting of information incidents. The management stated they are flexible with respect to training avenues (for example, providing online training, web-conferencing and classroom learning, where appropriate) with a view to increasing the number of trained government employees. The PIU desires further development of the training program but cites fiscal constraints as a limiting factor.

The BC Public Service Agency compiles privacy training completion rates and provides them to the OCIO. The OCIO, in turn, provides Ministry Chief Information Officers with training completion statistics on a quarterly basis. The rate of training completion for both executive and non-executive employees was 70.9% on July 31, 2014,[41] a slight decrease from the 73.8% completion rate of December 30, 2013.[42] While it may be difficult to achieve 100% completion due to staff turnover, leave and other reasons, considering the sensitive personal information collected by some of the larger government ministries, efforts to increase training completion rates are needed.

4.0 EXAMINATION FINDINGS

This portion of the report assesses the extent to which government ministries are complying with relevant sections of FIPPA, OIPC direction (as expressed through guidance documents, reports and orders) and government policies and procedures relating to privacy breach management. Report findings resulted from inspections of investigative files and interviews with OCIO and ministry staff. They consist of a statistical overview followed by an assessment in accordance with the OIPC's guidance with respect to responding to privacy breaches.

4.1 Breach Tracking, Statistics, Analysis and Reporting Out

As discussed above, the policy requiring privacy breach reporting to the OCIO commenced in 2010. Since then, the number of reported privacy incidents has increased considerably. Documentation of breach investigations has taken a variety of forms over the past few years. Originally, the PIU relied on Microsoft Excel spreadsheets for this work but, since 2013, the PIU has improved its case management system by utilizing a new system called "Perspective" by PPM2000.

Statistics provided by the PIU show that between April 1, 2010 and December 31, 2013, there were 3,779 suspected privacy breaches reported to the OCIO; of which 2,718 were found to be actual privacy breaches. See Table 1 for detail.

Table 1: Number of Suspected and Actual Privacy Breaches by Year

Year	Suspected	Actual	Sample
2010[43]	593	425	-
2011	958	626	-
2012	1,105	748	163
2013	1,123	919[44]	164
Total	**3,779**	**2,718**	**327**

Suspected breaches, actual breaches, and the sample of breaches are defined as follows:

- **Suspected breaches** (N=3,779) include all privacy-related incidents reported to the OCIO during the 2010 and 2013 calendar years;

- **Actual breaches** (N=2,718) are the 2010 to 2013 suspected breaches where the OCIO determined that personal information was indeed breached; and
- **Sample of breaches** (n=327) a sample of closed investigations of suspected breaches from the past two years (2012 to 2013) reviewed for this examination.

Across government ministries and agencies, the majority (83%) of actual breaches involve the personal information of government clients. Most breach incidents (72%) concern only one affected individual. Examples of the types of personal information breached include an individual's name and contact information, the fact that an individual is involved with a government program or service, date of birth and/or personal health number.

How are information incidents categorized and documented?

OCIO investigators categorized the majority of reported breaches as administrative errors. Administrative errors are considered by the OCIO to be minor in nature and often involve errors that government officials have made during the handling of government correspondence. They comprise nearly three-quarters (72%) of all actual privacy breaches from 2010 to 2013. Disclosure of personal information (verbal or otherwise) to individuals not authorized to receive it is the second most common category of suspected privacy breaches (16%). See Table 2 for a breakdown of the categories of privacy breaches and Appendix B for the PIU's privacy incident category definitions.

Table 2: 2010-2013 Actual Privacy Breaches by Category

Category	#	%
Administrative Error	1,949	71.7%
Disclosure	445	16.4%
Access	87	3.2%
Protection	76	2.8%
Lost	68	2.5%
Stolen	39	1.4%
Collection	27	1.0%
Other	16	0.6%
Cyber-attack	7	0.3%
Use	4	0.1%
Grand Total	**2,718**	**100.0%**

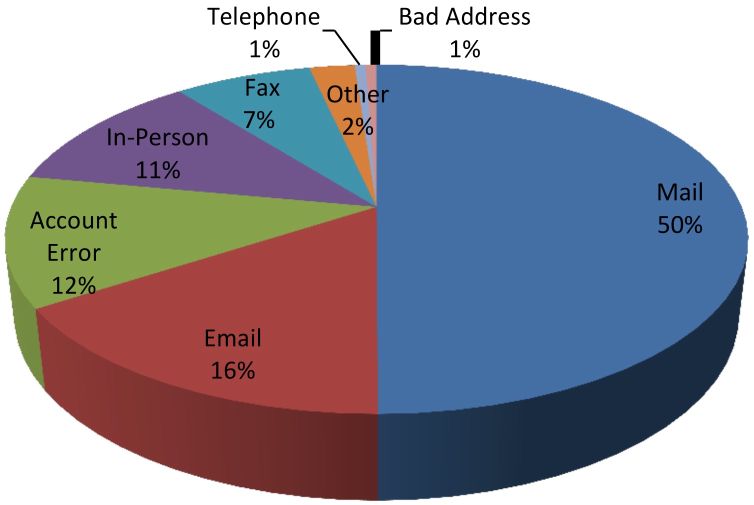
Other less common categories for privacy breach incidents include inappropriate access (3%), inadequate protection where reasonable security measures are not in place (3%), lost paper or electronic records (3%), stolen paper or electronic records (1%), inappropriate collection of personal information (1%), cyber-attacks of data systems through malicious code, hacking or phishing (<1%), and improper use of personal information (<1%).

The OCIO further breaks down administrative errors to identify the means by which the incident occurred (*e.g.,* via mail, email, in-person) and by the cause of the incident (*e.g.,* account error or bad address). These sub-categories and their prevalence are shown in Figure 1 below.

The most common sub-category of administrative errors, comprising half (50%) of all actual administrative errors from 2010 to 2013, consists of paper-based correspondence that is sent to, or received by, an unauthorized person. The OCIO notes that this sub-category often includes double-stuffed envelopes, lost mail, and other incidents where mail is the mechanism by which the records are transited.

Missent emails and account errors (derived from making changes to the wrong account) comprise the next two highest categories of administrative error (16% and 12%, respectively). Just over one-in-ten privacy breaches from 2010 to 2013 occurred in-person where personal information was physically handed to an unauthorized person during an interaction, such as a cheque or other documents being issued to the incorrect individual.

Figure 1: 2010-2013 Actual Administrative Errors by Sub-Category



Over the course of the examination, the OIPC examination team found some inconsistencies in the tracking and analysis of information incidents and privacy breaches within the government:

- It was not immediately clear whether there is a substantive distinction between an incident classed as an administrative error as opposed to being classed as a disclosure, and the tracking of the category of incident was not always consistent. In other words, sometimes a particular type of incident was noted as an administrative error, while another similar incident was categorised as an unauthorized disclosure. The confusion may derive from the possibility that an incident can be both an unauthorized disclosure and it could have occurred as a result of an administrative error. The categories are not mutually exclusive and there appears to be overlap in both the definitions of the categories and sub-categories, as well as tracking documentation within breach files.
- Category definitions do not always accurately reflect how the category is applied. For example, the OCIO defines administrative errors as "incidents that are minor in nature and involve errors as a result of the inappropriate handling of government correspondence....".[45] However, OIPC examiners were of the opinion that a number of the breaches categorized as administrative errors were not "minor in nature" and found that half of the OCIO investigations that were lengthy were categorized as administrative errors. In addition, the OCIO defines account errors as updating a person's account with the information of another person, but without there being any disclosure of personal information to anyone. However, some breach files categorized as account error involved cases where disclosure did occur.
- It was unclear why some breaches were deemed non-government breaches when the party responsible for an incident was identified as a ministry or service provider. While there may be explanations for specific cases, there were others where OIPC examiners were of the view that the breach may have been inappropriately identified as non-government. Errors in this regard may affect the counting of actual breaches and could result in the number of government breaches being higher than currently reported. Such errors may also affect decisions regarding notification of individuals or reporting to the OIPC.

The number of actual breaches by ministry from 2010 to 2013 appears in Table 3 below. The four ministries with the largest numbers of breaches (SDSI, MoH, MCFD and JAG) process a large volume of sensitive personal information. Consequently, these four ministries also have the largest numbers of administrative errors. These errors often relate to the processing of personal information via mail.

Table 3: Number of Actual Privacy Breaches 2010-2013 by Ministry

Ministry	#	%
Social Development and Social Innovation	848	31.2%
Health	653	24.0%
Children and Family Development	371	13.6%
Justice	354	13.0%
Technology, Innovation and Citizens' Services	150	5.5%
BC Public Service Agency	116	4.3%
Finance	90	3.3%
Forests, Lands and Natural Resource Operations	28	1.0%
Jobs, Tourism and Skills Training	23	0.8%
Energy and Mines	22	0.8%
Advanced Education	17	0.6%
Education	11	0.4%
Other[46]	35	1.3%
Grand Total	**2718**	**100.0%**

What types of analyses and reporting are conducted regarding breaches?

The Ministry of Technology, Innovation and Citizens' Services published breach statistics for the first time in their *2012/2013 Annual Report on the Administration of FIPPA*. However, there appears to be little analysis and reporting regarding breach incidents and statistics available to the public are limited.

Ministry information and security staff from three of the four ministries studied indicated that they conduct additional analysis of breach incidents internally. One good practice noted was that SDSI conducts a more advanced analytical and reporting function. SDSI staff track and analyze all incidents, including categorizing each incident to determine the severity or risk level. They keep a register of the following:

- number of incidents with year;
- category or type of breach;
- division within SDSI;
- regions;
- severity of the breach;
- notification of affected individuals and OCIO; and
- timelines from discovery to reporting.

Information and security staff keep the electronic register up to date and use it to create charts and graphs for executive reporting and informing staff. Analysis of this information helps SDSI to identify whether there are problem areas within particular divisions or regions and to target specific issues to the unit or office accountable.

While some ministries are conducting useful analysis, the OCIO does not appear to be conducting the same level of analysis on the centralized information on privacy breaches. This means that the OCIO may be missing opportunities for shared learning and for addressing root causes of privacy breaches within government.

Are audits of privacy controls conducted?

In addition to a limited amount of analysis and reporting out of breach incidents across government, staff from the four ministries reviewed indicated that there were no regular internal audits being conducted of their ministry or service providers' privacy and security controls. Certain ministries, including SDSI and MoH, indicated that they have embarked on the planning of security audits, including selection of audit targets, the development of procedures and the formulation of audit methodology, but have not conducted formal internal audits yet.

The OIPC's *Accountable Privacy Management in BC's Public Sector*[47] states that internal audits of security safeguards should form a key component in a public body's privacy management program. An effective internal audit program will also allow a public body to determine whether they are complying with their duties under s. 30 of FIPPA to protect personal information against unauthorized access or disclosure. Audits of service providers are also necessary to ensure that appropriate safeguards are in place and that service provider employees are trained accordingly.

In summary, gaps were found in the tracking, statistics, analysis and reporting out of breaches within the government. There are also no regular internal audit activities to ensure adequate safeguards are in place. Enhancing privacy compliance monitoring activities within the breach management program is essential for fostering an environment of accountability and transparency.

4.2 Breach Containment

When a privacy breach occurs, public bodies must make every reasonable effort to recover the personal information. In the sample of files, the majority of breaches (75%) were discovered right away or within a day of the suspected breach occurring. Once a breach has been discovered, the first step is an immediate attempt to contain the breach by stopping the unauthorized disclosure or access, recovering the records, correcting weaknesses in security and ensuring that compromised records are appropriately destroyed. The OIPC breach guidelines also point to immediately contacting the privacy officer and the person responsible for security within the organization.

Are efforts made to contain the breach and/or recover records?

The government contained actual breaches in 86% of the sampled files. The cases where the breach was not contained often involved misdirected mail, incidents of lost and stolen data and verbal disclosures. In these cases, attempts were made to notify affected individuals or the OCIO documented that notification was not required due to low risk or no risk of harm to individuals as a result of the breach.

Are breaches reported to the OCIO?

As noted above, government employees must report all actual or suspected information incidents to the OCIO.[48] PIU staff and key contacts from select ministries reported believing that there is 95% or greater compliance with the government's policy on mandatory reporting to the OCIO. However, it was not possible to determine objectively the precise statistical level of compliance with this policy.

The four ministries reviewed each track information incidents related to their individual ministries in addition to reporting them to the OCIO, but there were many data quality issues that caused discrepancies between the list of breach incidents recorded by the OCIO compared to the lists provided by the ministries. For example, one database did not record a unique identifier for each breach, making precise direct comparisons impossible. In other cases, the OCIO file numbers identified in a particular ministry's list were associated to a different ministry in the OCIO list. There were also cases where there was not enough information included in one of the databases to be able to compare to the other.

Are breaches reported to the OCIO in a timely fashion?

The OIPC *Privacy Breaches: Tools and Resources*[49] recommend reporting breaches to the privacy officer within the public body on the same day that the breach was discovered. Similarly, the government's *Process for Responding to Privacy Breaches* notes that these incidents must be reported "immediately".

Based on a review of timelines within the sample of suspected breaches, individuals reported the majority of breaches (80%) to the OCIO on the same day or the day after the incident was discovered. Another 9% were reported within 3-5 business days; and 11% from one week to one month after the breach incident was discovered. This means that 20% of incidents were not reported "immediately". Delay in reporting breaches to the OCIO may impact the timeliness of the essential elements of breach management.

Are investigations of suspected breaches occurring in a timely fashion by the OCIO?

Across all categories of breaches contained in the sample, OCIO investigations took an average of less than one month to complete. OCIO investigators closed 36% of all sampled files within two business days of the incident being reported. Within two weeks, investigators completed 60% of files, and, by the end of one month, 72% of all investigative files were closed. Thirteen percent took longer than two months to investigate. While some of these appeared to constitute larger or more complex files, half of the lengthy investigations files were categorized as administrative errors.

4.3 Risk Evaluation

Effective privacy breach management includes determining what additional steps (such as notification of individuals, reporting to the OIPC, or developing preventative measures) are necessary. This process is described as a "risk evaluation" by the OIPC and as an "assessment of the extent and impact" by the OCIO. Regardless of the title, this step appears to involve a process that attempts to evaluate the link between the personal information involved in the breach and the circumstances in which it was disclosed or accessed, to determine whether the breach may harm the involved parties.

Some of the factors that OCIO investigators consider as part of this process include:

- Sensitivity of the personal information;
- Level of containment;
- Steps that have already been taken to minimize harm;
- Systemic issues;
- Type and number of individuals affected;
- Physical harm or threat to physical well-being;
- Identity theft or fraud;
- Financial loss;
- Loss of employment or business opportunities;
- Contractual obligations;
- Hurt, humiliation or embarrassment;
- Loss of trust;

- Loss of assets;
- Financial exposure;
- Loss of contracts or business; and
- Risk to public health or safety.[50]

Most decision makers understand the tangible damages such as physical and financial harms that could result from breaches. However, there is also the potential for intangible distress that needs to be considered by those who conduct these risk evaluation processes. Examples of intangible distress may include reputational harm, personal, family, workplace or social fear, embarrassment, apprehension or anxiety, unacceptable intrusion into private life, and discrimination or stigmatization.[51]

What types of harm were identified in BC Government breaches?

Overall, the most common type of harm to individuals identified within the file sample was hurt, humiliation, damage to reputation or credibility of individuals.[52] The potential for harms to the individual such as identity theft, financial loss or physical harm appeared in less than 10% of the files.

Other types of harm identified – but unrelated to considerations for notification of affected individuals – included damage to reputation of government and the potential for future breaches due to similar systemic failures.

How was risk evaluation conducted?

While the OCIO policies outline considerations for assessing the extent and impact of a privacy breach, and acknowledging that these assessments or evaluations can be difficult, it is not clear how one is to actually determine whether a foreseeable harm exists.

Some records did include notation stating that the probability of harm was low or high (and, hence, included a recommendation to the ministry to notify or not to notify affected individuals). However, OIPC examiners were not able to reliably evaluate how PIU investigators conducted the assessment. Of note, the personal information at issue was not identified in some of the sampled files.[53] In order to appropriately evaluate the extent and impact of a privacy breach, the personal information involved in the breach needs to be identified, documented and considered.

Privacy risk evaluation is a difficult exercise because the unique circumstances and context for any given privacy breach can be so variable. The sensitivity of the information is not the only consideration. It is also important to explore the potential uses for the information and who might have had access to it. OCIO policies (as well as OIPC guidelines) do not provide direction as to how to actually conduct the risk evaluation process. There needs to be explanation of how to draw a connection between the personal information involved and the types of harm the individual could suffer from the breach, the probability or likelihood of that harm occurring, and the severity of harm if it did occur.

In addition, there is no instruction on how the results of the risk evaluation process are to be used in determining whether to notify individuals or what steps should be taken to contain the breach or prevent further occurrences. These decisions may become highly subjective in the absence of such direction.

4.4 Notification and Reporting

4.4.1 Notification of Affected Individuals

As noted above, part of a public body's duties under s. 30 of FIPPA include determining whether affected individuals should be notified. Notification of affected individuals can be an important mitigation strategy. Public confidence in the government's collection and use of personal information is strengthened when notifications to affected individuals are provided in appropriate cases.

The OIPC guidelines indicate that notification should occur as soon as possible following a privacy breach and within one week following the discovery of the breach.[54] In order for notification to be effective and to constitute reasonable security, it must be given in a timely enough fashion to allow those notified to mitigate harm. As previously mentioned, an inappropriate delay of notification of affected individuals was considered in Investigation Report F08-02 to be a failure by the public body to meet its s. 30 obligations.[55]

When should affected individuals be notified?

This examination found that there is no specific threshold that delineates the point at which public bodies need to notify individuals affected by a privacy breach. As noted above, the government's *Process for Responding to Privacy Breaches* identifies the key consideration for making this determination is whether notification is necessary to mitigate harm to an individual. Other considerations listed in the government's policy include legislative requirements, contractual obligations, and a loss of citizen's confidence in government.[56] The PIU Director noted that determining whether affected individuals should be notified can be complex. The general practice is to base notification to individuals on a "balance of harms" principle. According to the IIMP*:*

> Under this principle, an individual(s) who could potentially face harm as a result of an information incident may not be notified if it is determined that the harm that would result from conducting notification would outweigh the benefit to be gained from the notification.[57]

OCIO investigative staff noted during interviews that the decision-making processes for whether to notify affected individuals has changed over time. Currently an investigator must seek the PIU Director's approval before recommending that a ministry notify affected individuals. The reported purpose of this change is to avoid over-notification in cases where the breach poses no risk of harm to the individual.

Are individuals notified when their personal information has been breached?

The OCIO determined notifications of affected individuals to be required in 40% of all actual breaches from 2010-2013. Based on available evidence, this examination did not uncover any circumstances within the sample of investigative files where OIPC examiners thought notification should have been provided but was not provided.

Within the sample of breaches, 71 files met the OCIO's criteria for notification. There were additional files where the OCIO did not determine that notification was required, but the ministry decided to notify regardless. Notification of affected individuals occurred or was attempted in 85 files.

The majority of notifications from the sample (65%) were provided verbally or in person. Letters were sent in 19 cases (22%). Notifications were unsuccessful in seven cases (8%), most commonly due to an inability to locate the individual. In one case, a note was added to the client's file to alert the individual during the next client interaction. In another case, after consulting with professionals involved in the client's care, the OCIO determined that notification could cause the client undue harm or distress and opted not to notify. Information on a further two files was either unclear or missing from the sample data. These four examples comprise the remaining 5% of notifications in the sampled files.

Are individuals notified in a timely fashion?

There were insufficient numbers of files containing notification letters to be able to reach statistical conclusions with confidence. As noted above, the database of sampled files indicated that written notifications were sent to affected individuals in 19 cases. However, only 11 letters were included in the OCIO files and available for review. Of these 11 files, six files were excluded from analysis for various reasons (for example, as earlier verbal notification had been provided), leaving only five notification letters for review.

Despite the number of notification letters being insufficient to reach conclusions with confidence, delay was noted in each of the five cases, ranging from 7 to 39 business days. As the purpose of providing notification is to mitigate the harm of identity theft, financial loss and/or other harms, the default should be early notification and public bodies should not, without appropriate reason, delay notification.

Are notifications adequately conveying essential information?

The OCIO provide direction and messaging for ministry staff to use when providing verbal or written notifications. OCIO records indicate that the majority of notifications were provided either by telephone or in person and, as such, the examination team was unable to review the content of the majority of notifications. The five letters that were available for review contained all of the essential elements of a notification letter.

The OIPC's privacy breach guidance document and the Government's *Process for Responding to Privacy Breaches* both set out the essential elements of what should be contained in a privacy breach notification letter.

Notifications should include the following pieces of information:

- Date of the breach;
- Description of the breach;
- Description of the information inappropriately accessed, collected, used or disclosed;
- Risk(s) [of harm] to the individual caused by the breach;
- The steps taken so far to control or reduce the harm;
- Future steps planned to prevent further privacy breaches;
- Steps the individual can take to further mitigate the [potential for] harm (*i.e.,* how to contact credit reporting agencies to set up a credit watch, information explaining how to change a personal health number or driver's license number);
- Contact information of an individual within the public body or organization who can answer questions or provide further information; and
- Privacy Commissioner contact information and the fact that individuals have a right to complain to the Office of the Information and Privacy Commissioner. If the public body or organization has already contacted the Privacy Commissioner, include this detail in the notification letter.[58]

While available evidence suggests that affected individuals received notification in order to assist in harm mitigation, it is important for the OCIO to ensure they receive and review copies of notification letters to ensure effective management of this process.

4.4.2 Reporting to the OIPC

As noted above, reporting breaches to the OIPC is an important consideration for public bodies to manage privacy breaches and meet their duties under s. 30 of FIPPA. Effective oversight by the OIPC increases public trust and confidence that the government is appropriately managing and safeguarding personal information. Open, accountable and transparent communication with the OIPC, particularly with regard to reporting breaches that occur, is key to the oversight function and is in the public interest.

The Commissioner expects prompt reporting of privacy breaches to the OIPC in cases where reporting is appropriate.[59] The OIPC privacy breach guidelines state that determination of whether it is appropriate to report the breach to the OIPC should be made "generally within 2 days" of the breach.[60]

As noted above, the *Process for Responding to Privacy Breaches* policy states that the OCIO is solely responsible for liaising with the OIPC regarding an actual or suspected privacy breach. However, individual ministries are ultimately accountable for compliance with s. 30 of FIPPA. PIU staff advised that they make decisions to report to the OIPC on a case-by-case basis and include discussion with ministry clients and consideration of the OIPC's breach guidance document. Most of the ministry information and security staff interviewed for this examination noted they rely on the OCIO's discretion and lead for whether to report to the OIPC.

Both citizens and public bodies benefit from the reporting of breaches to the OIPC at the earliest stages of breach management. The OIPC is well placed to help as it has broad knowledge and expertise from both public and private sector experiences. With this knowledge and expertise, the OIPC provides independent and expert guidance on the management of breaches that is best suited to the needs of those involved.

When should public bodies report breaches to the OIPC?

FIPPA does not include an explicit requirement for public bodies to report breaches to the OIPC. OIPC privacy breach guidelines and the *Process for Responding to Privacy Breaches* set out factors to be considered in reporting a breach to the OIPC. These factors are similar to those listed for conducting risk evaluation and add the existence of systemic problems as an indicator of when it would be appropriate to notify the OIPC. These factors are helpful in balancing the different considerations about when to report to the OIPC but do not provide a standard measure that clearly delineates when reporting to the OIPC should occur.

As such, this examination found that there is no specific threshold that triggers a need for public bodies to report breaches to the OIPC. The decision of whether to report ends up being very subjective. A more definitive measure would provide a greater level of certainty to ministries. A clear standard could help ensure greater consistency in breach reporting and give public bodies' greater confidence that their decisions would comply with s. 30 of FIPPA.

Reviewing examples from other jurisdictions may be useful in forming the basis for a clear measure for use by the public sector in British Columbia.

For example, in Ottawa, the Treasury Board of Canada Secretariat ("TBS") issued a directive effective May 6, 2014, making it mandatory for all material privacy breaches involving sensitive personal information to be reported to the Office of the Privacy Commissioner of Canada ("OPC"), to the TBS and to parties affected by the privacy breaches. The accompanying TBS *Guidelines for Privacy Breaches* define "material breaches" as breaches that involve "sensitive personal information, and could reasonably be expected to cause serious injury or harm to the individual and/or involves a large number of affected individuals".[61]

For the private sector, the Government of Canada introduced Bill C-12 that, if passed, would require businesses to report any "material breach of security safeguards" involving personal information under their control to the OPC.

In addition, Alberta has legislation that requires private sector organizations to report to the Alberta OIPC when a privacy breach results in a "real risk of significant harm".

These breach reporting models appear to differ in terms of the thresholds for reporting to the oversight authority, suggesting that it is difficult to establish a threshold that would work in all cases. As such, further experience may be needed to determine which model of breach reporting would be most effective in practice.

Regardless, whether imposed by statute or government policy, British Columbia would benefit from public bodies receiving more specific and less subjective direction as to when to report to the OIPC (and when to notify affected individuals) about breaches, and would increase public confidence that personal information is being managed properly.

Public bodies would also benefit by receiving a description of the proper methodology for evaluating the privacy harm that may result from a breach. This should include direction about establishing a connection between the disclosure of the information and the types of harm that might result, as well as the likelihood of that harm occurring, and the severity of harm if it did occur.

Are breaches reported to the OIPC?

The examination team was unable to verify when sampled files were reported to the OIPC because there was minimal cross-referencing and recording of the corresponding OIPC file number. However, based on the review of the sampled files, OIPC examiners were of the opinion that a small number (2%) of the sampled files should have been reported to the OIPC. Reasons why these cases were identified for forwarding to the OIPC include the sensitivity of the personal information, the potential for harm, lack of containment, systemic issues, high profile incidents and those involving potential criminal charges.

It is important to note that OIPC breach guidance documents recommend that determination of whether to report to the OIPC should be made within two days of discovering a breach. The examination team made determinations on files after the investigation was completed. Had the examination team reviewed files at the two-day mark when less information was available (for example, regarding containment), it is likely that a greater number of files should have been reported to the OIPC.

Are breaches reported to the OIPC in a timely fashion?

Data was not available to determine the timeliness of reporting to the OIPC.

4.5 Prevention Strategies

After taking initial steps to contain the breach and mitigate potential harms associated with the breach, public bodies should conduct more in-depth analysis with a view to preventing future breaches. OIPC guidance documents point to a review of policies and procedures; an audit of physical and technical security; training; and an eye toward long term safeguards as ways to minimize the potential for further breaches.[62] Examples of preventative measures may include changes to public body policies or procedures, improved physical security, enhanced technological security, training for staff or service providers, and changes to supervision and/or contracts with service providers or other contractors.

Are preventative measures being identified?

Preventative measures appeared in 90.8% of all actual breaches[63] contained within the sample of breach investigation files. The most common types of preventative measures across all sampled files included:

- Staff coaching and additional training (72.5%);
- Changes to practices, procedures or business processes[64] such as instituting double-checking procedures, changes to protocols for

transporting information or for vetting files, reminders to team members to practice caution (11.3%);

- Technological changes such as amending security or access controls in information systems (1.2%); and
- Updating internal policies (0.6%).

The OCIO only issued mandatory recommendations in one of the sampled files, meaning that the vast majority of recommendations provided by the OCIO to the ministries were advisory recommendations. As noted earlier in this report, according to the IIMP, "mandatory" recommendations must be implemented, while it is the ministry's discretion whether to implement "advisory" recommendations.

Are preventative measures being implemented?

The sample files reviewed did not often contain evidence that follow-up or implementation of preventative measures occurred. While PIU investigators reported believing that recommendations are being implemented, they noted that they do not monitor implementation because of time restrictions and heavy workload. PIU management said that they would like to track implementation of preventative measures in a more thorough manner, but indicated that there were limited resources to do so.

Government policy does not require ministries to follow-up with the OCIO about implementation of "advisory" recommendations which represent 99% of recommendations made by the OCIO. Part of effective privacy breach management, however, includes confirming that preventative measures are fully implemented to ensure the lessons learned are incorporated into procedures, practices and employee training.[65]

5.0 DISCUSSION AND RECOMMENDATIONS

The examination has revealed that the government has a solid foundation in place for managing privacy breaches. Since the government's centralization of the information incident management process within the OCIO in 2010, government employees have reported over 4,500 suspected breaches to the OCIO. On average, the OCIO receives and investigates an additional 10% of suspected privacy breaches each year.

In general, this examination found that the reporting of suspected breaches to the OCIO occurred within a day or two of discovering the incident, government contained the majority of breaches, and the OCIO investigated them within a reasonable timeframe. In addition, ministries provided notifications to affected individuals when appropriate, and the written notifications examined included all of the necessary information. The OCIO also provided advice on preventative measures in almost every investigation.

There are, however, opportunities for improvement. An effective, accountable privacy management program needs more than a solid foundation. The government should consider addressing the gaps cited in this report by leveraging the advantages of the centralized breach management model. They should also consider adopting a structure that reduces the subjectivity of determining when to notify affected individuals and the OIPC.

Finally, government should work to continually improve breach management processes and to increase education and awareness. Together, these changes would build on the existing strengths of the current privacy management program.

Leverage opportunities of centralization

Presently the privacy program appears to be primarily focused on managing responses to individual breaches, and does not utilize available information to achieve long term solutions.

For example, there is minimal analysis of breach incidents across government. There appears to be no identification of systemic issues and the root causes of breaches. There is also limited reporting about breaches in general and limited information available to the public regarding government breaches. Finally, neither the OCIO nor the four ministries reviewed currently conduct regular proactive audits internally or of their service providers with regard to privacy and security provisions, including breach management.

The OCIO has a centralized repository of information about breaches. This means that the OCIO is well-positioned to conduct audits and analysis that would improve compliance with government-wide policies. This also presents the OCIO with a unique opportunity for cross-government monitoring of privacy breaches to:

- analyze the root causes of privacy breaches and identify potential solutions that may aid in preventing future breaches;
- ensure compliance with government's policies on collection, use and disclosure of personal information and how to respond in the event of a breach;

- provide information and expertise to the ministries regarding how best to safeguard the personal information they collect; and
- provide information to the public regarding the protection of their personal information.

The OIPC public sector accountability guideline recommends that public bodies employ an internal audit program that evaluates and reports on compliance, along with external audits where a larger public body has suffered a significant privacy breach. Establishing a compliance monitoring program is a vital step in an effective and accountable privacy breach management program. The OIPC recognizes that additional resources may be required to perform and maintain this function, and states that annual budgets should reflect shifting needs for compliance resources.[66]

Effective monitoring of the privacy breach program includes compliance monitoring and analysis of ministry, service provider and employee adherence with relevant policies. It also involves identifying causes of breaches, systemic trends and potential preventative measures. This examination found that 20% of breaches were not reported to OCIO immediately or within two days, there was a delay in notifying affected individuals in some cases, and there is limited follow-up with ministries on the implementation of OCIO recommendations. An effective privacy compliance monitoring function may have identified and resolved these issues.

Communication of compliance monitoring and analysis is also an important part of privacy breach management. This helps to ensure that ministries and individual staff have learned relevant lessons and incorporated them into procedures, practices and employee training, or taken corrective measures where appropriate. In addition, detailed public reporting of privacy breach information (whether in individual or aggregate form) would increase transparency, accountability and public confidence.

In summary, government is currently missing opportunities inherent in a centralized model. Examining how personal information and breaches are managed and contributing to shared learning about privacy safeguards, effective breach responses, and preventative measures would provide important benefits. Creating an ongoing privacy compliance monitoring function would foster accountability within the privacy management program and would increase public confidence.

RECOMMENDATION 1:

The Government of British Columbia establish an ongoing privacy compliance monitoring function within the OCIO that:

a) Reviews processes, policies and training government-wide, to ensure that breaches are promptly reported to the OCIO and that affected individuals are notified without delay;

b) Conducts regular follow-up with ministries to ensure full implementation of prevention strategies and recommendations provided through the breach investigation process;

c) Reviews privacy and security safeguards within ministries and service providers;

d) Conducts regular cross-government analysis of the causes and potential solutions to privacy breaches; and

e) Publicly reports detailed information relating to breaches, bodies responsible, types and causes, and preventative measures annually.

Risk Evaluation, Notification and Reporting

The OIPC expects that public bodies, as part of their FIPPA duty to protect personal information, will promptly report privacy breaches to the OIPC and notify affected individuals where appropriate.[67] It is the risk evaluation process that helps to determine when this notification and reporting should occur.

This examination found that risk evaluation processes lack clarity, which leave decisions regarding how to manage a breach highly subjective. In addition, there is no clear standard that triggers the need for notification and reporting. There is a need for more definitive and measurable indicators, tied to risk evaluation processes, to be entrenched in legislation or government policy.

Establishing a standard risk evaluation process and definitive measures for notification and reporting is difficult. Jurisdictions across the world have been grappling with this problem for many years, and there is a lack of consensus as to the best models and thresholds for notification and reporting. There is variability in interpretation and application of concepts such as “real risk of significant harm” or “material breach”, as both require an assessment of the privacy-related risks and harms.

In addition, it is difficult to balance the tensions between the actions necessary to address the potential harm to affected individuals and the implication of these actions on the parties involved (including individuals, public bodies and regulators). An optimal balance will not be able to be achieved until additional research has been conducted and other models tested.

In the meantime, we propose that the government, on an interim basis, **report all suspected breaches to the OIPC if the suspected breach involves personal information, and could reasonably be expected to cause harm to the individual and/or involves a large number of individuals**.

While similar to the model established by the TBS whereby material breaches are to be reported to the TBS and OPC, this interim standard will assist public bodies in deciding when to report breaches to the OIPC. This interim standard is intentionally set as a lower threshold than the TBS model in order to allow the OIPC to receive more breach reports to aid in evaluating breach reporting models.

However, considering that current reporting of breaches to the OIPC is open to various interpretations, it remains to be seen how this interim standard will impact the actual number of reports to the OIPC. See Appendix C for examples that illustrate the interim standard.

As well, ministries are not prevented from reporting breaches to the OIPC that fall short of the interim standard. This could be helpful for ministries as the OIPC has considerable experience assisting public bodies and private sector organizations in responding to and managing privacy breaches.

Implementation of this interim standard would provide an opportunity for the OIPC and OCIO to evaluate the model to determine its appropriateness, not only for ministries, but also for the public sector as a whole.

The OIPC will continue to research and monitor issues related to privacy breach management, including potential amendments to FIPPA in the area of public sector breach notification and reporting requirements. The OIPC is also committed to amending the privacy breach guidelines to clarify expectations relating to privacy breach reporting and privacy breach management in general.

RECOMMENDATION 2:

The Government of British Columbia to adopt the following interim breach reporting requirements:

a) Document risk evaluation processes and decisions regarding notification of affected individuals and reporting to the OIPC; and

b) Report all suspected breaches to the OIPC if the suspected breach:
   - involves personal information; and
   - could reasonably be expected to cause harm to the individual and/or involves a large number of individuals.

Breach Management Processes

Overall, findings suggested that the fundamentals of breach management in the BC Government are being managed well. However, there were some inconsistencies in the tracking and information available about breach incidents. The examination uncovered inconsistencies in the following:

1. Breach categorization (for example, there appears to be overlap between the categories of administrative errors and disclosures);
2. Definitions of breach categories (for example, not all breaches marked as administrative errors were found to be minor in nature, and some breaches noted as account error were applied to circumstances where disclosure occurred);
3. Tracking of party responsible (for example, a contracted service provider may be recorded as an external organization, a service provider, or as "other" and may be inappropriately identified as non-government);
4. Identification of personal information during reporting, triage or investigation (for use in evaluating the risk of harm to individuals following a breach);
5. Tracking of notification dates (for both verbal and written notifications);
6. Collection and retention of breach notification letters;
7. Ministry tracking of the OCIO file number; and
8. OCIO tracking of OIPC file number.

The OCIO should re-examine how it categorizes breaches. It needs to draw distinctions between (1) the type of breach (*e.g.,* FIPPA s. 30 unauthorized access, collection, use, disclosure or disposal) from (2) the cause of breach (*e.g.,* fraud, stolen, cyber-attack, lost, administrative error) and from (3) the method of data transfer (*e.g.,* mail, telephone, email, in-person).

It is also important for ministry and OCIO staff to document the responsible parties and other details about information incidents correctly and completely. Fulsome documentation of breaches will assist the OCIO in effectively assessing risk of harm in individual breaches, in determining when to provide notifications to affected individuals and to the OIPC, in identifying systemic issues to mitigate reoccurrence, and in providing centralized governance of the BC Government's breach management process.

Changes made to process and documentation procedures need to be reflected in policy and communicated to relevant government staff. The OIPC's *Accountable Privacy Management in BC's Public Sector* states that a public body should "monitor, assess and revise its privacy management program regularly and consistently" in order to ensure it meets its FIPPA obligations.[68] PIU management noted during interviews that plans are already in place to update and enhance cross-government breach management policies and training.

RECOMMENDATION 3:

The Office of the Chief Information Officer to:

a) Review and amend breach categories and category definitions;

b) Ensure fulsome and accurate collection and documentation of privacy breach incidents;

c) Ensure ministry tracking of the OCIO file number; and

d) Ensure OCIO tracking of the OIPC file number.

RECOMMENDATION 4:

The Office of the Chief Information Officer to:

a) Review and amend policy documents relating to privacy breach management; and

b) Provide basic guidance or training for privacy breach investigative staff as well as ministry information and security staff relating to amendments made.

Education and Awareness

As discussed above, the privacy training completion rates for government employees and executives have dropped slightly to just over 70%. Higher privacy training completion rates are warranted given that the government has mandated privacy training, and that government programs and service providers collect very sensitive personal information. This training should include the importance of protecting personal information, an overview of breach management process, and the OCIO's role. This would assist in ensuring that:

- staff are aware of their obligation to protect personal information;
- all suspected breaches are reported to the OCIO in a timely fashion;
- breaches are managed properly when they do occur;
- notifications to affected individuals occur without delay; and
- breaches are appropriately reported to the OIPC.

PIU staff cited a need for ongoing refresher training for government employees regarding the protection of personal information and breach management processes. PIU management noted that government staff are ready for a more robust training program.

The OIPC's *Accountable Privacy Management in BC's Public Sector* notes that:

> Training and awareness are necessary because, in order for a privacy management program to be effective, employees must be actively engaged in privacy protection. Employees will be able to better protect privacy when they are able to recognize privacy issues as they arise. A public body may have sound privacy controls in place, but if employees are not aware of them, the controls are of no real use. An effective privacy management program will enable all employees and officials to be aware of, and be ready to act upon, the public body's privacy obligations. If an urgent need arises, prompt communication of essential information must be disseminated to relevant employees as soon as is practical, without waiting for the next organized training session.
>
> Privacy training should be mandatory for all employees, and should be tailored to their specific duties. Training should be ongoing, regular and sufficiently detailed and informative as to equip employees with the knowledge (and awareness) necessary to meet the public body's privacy obligations. The content of the training program should be periodically revisited and updated to reflect changes within the public body, to FIPPA and to industry best practices.[69]

RECOMMENDATION 5:

The Government of British Columbia to:

a) Provide ongoing training and awareness of the importance of protecting personal information and breach management processes; and

b) Increase staff (and service provider, if applicable) participation rates in this training.

6.0 SUMMARY OF RECOMMENDATIONS

RECOMMENDATION 1

The Government of British Columbia establish an ongoing privacy compliance monitoring function within the OCIO that:

a) Reviews processes, policies and training government-wide, to ensure that breaches are promptly reported to the OCIO and that affected individuals are notified without delay;

b) Conducts regular follow-up with ministries to ensure full implementation of prevention strategies and recommendations provided through the breach investigation process;

c) Reviews privacy and security safeguards within ministries and service providers;

d) Conducts regular cross-government analysis of the causes and potential solutions to privacy breaches; and

e) Publicly reports detailed information relating to breaches, bodies responsible, types and causes, and preventative measures annually.

RECOMMENDATION 2

The Government of British Columbia to adopt the following interim breach reporting requirements:

a) Document risk evaluation processes and decisions regarding notification of affected individuals and reporting to the OIPC; and

b) Report all suspected breaches to the OIPC if the suspected breach:

- involves personal information; and
- could reasonably be expected to cause harm to the individual and/or involves a large number of individuals.

RECOMMENDATION 3

The Office of the Chief Information Officer to:

a) Review and amend breach categories and category definitions;

b) Ensure fulsome and accurate collection and documentation of privacy breach incidents;

c) Ensure ministry tracking of the OCIO file number; and

d) Ensure OCIO tracking of the OIPC file number.

RECOMMENDATION 4

The Office of the Chief Information Officer to:

a) Review and amend policy documents relating to privacy breach management; and

b) Provide basic guidance or training for privacy breach investigative staff as well as ministry information and security staff relating to amendments made.

RECOMMENDATION 5

The Government of British Columbia to:

a) Provide ongoing training and awareness of the importance of protecting personal information and breach management processes; and

b) Increase staff (and service provider, if applicable) participation rates in this training.

7.0 CONCLUSION

Effective privacy breach management forms part of public bodies' duties to protect personal information as contemplated by s. 30 of FIPPA. The government centralized its privacy breach management process within the OCIO. This centralized model for privacy breach management has developed into a solid foundation and now provides a unique opportunity for the OCIO to leverage the benefits of centralization.

This examination has highlighted a need for compliance monitoring, public reporting, follow-up on implementation of preventative measures, fulsome and accurate documentation and categorization of privacy breaches, and increased training participation rates. The OCIO and ministries can address these needs by implementing the recommendations included in this report, along with the provisions contemplated in the OIPC's *Accountable Privacy Management in BC's Public Sector*. The establishment of an ongoing privacy compliance monitoring function would foster accountability within the government's management of that personal information.

The government and the OCIO in particular as the centralized governance for privacy breach management, need to lead the creation and maintenance of a culture of privacy awareness and accountability. Together, these changes would build on the existing strengths and effect a maturation of the government's overall privacy management program.

In addition, an interim standard for reporting to the OIPC was recommended in order to be able to further consider the circumstances, criteria and methods for conducting risk evaluations and to determine the appropriate thresholds for reporting and notifications. While appreciating the inherent difficulty, continued efforts must be made toward finding an optimal balance between strict and potentially costly reporting and notification requirements versus the privacy rights of individuals and the mitigation of privacy harms.

8.0 ACKNOWLEDGEMENTS

The Government of British Columbia, the OCIO and selected government ministries cooperated fully with this examination.

Thank you to Tanya Allen, Senior Investigator and Tina Doehnel, Investigator for conducting this examination and assisting in drafting this report.

January 28, 2015

ORIGINAL SIGNED BY

Elizabeth Denham
Information and Privacy Commissioner
for British Columbia

9.0 APPENDICES

9.1 Appendix A: Methodology

As noted above, the scope of the examination included:

1. **OCIO Process Review**: a review of relevant OCIO policies and procedures;
2. **File Review**: an inspection of OCIO investigative files and other relevant information; and
3. **Ministry Processes Review:** a review of processes within select ministries where breaches have occurred.

OCIO Process Review

This review and the subsequent reporting included an overview of the mandate of the OCIO; interviews with staff and management; analysis of the policies and procedures that define how information incidents and privacy breaches are to be managed; developing an understanding of the investigative process undertaken once a privacy breach has been reported to the OCIO; and an overview of the mandatory privacy training provided to BC Government staff.

Materials reviewed for this portion of the examination included:

- Copies of relevant legislation, policies and procedures;
- Statistical summary of OCIO information incidents;
- Organizational charts;
- Descriptions of roles and functions for OCIO units and staff;
- Internal reviews of relevant privacy breaches;
- Ministry of Technology, Innovation and Citizens' Services Annual Reports;
- BC Government General Services Agreement;
- Copies of relevant OIPC guidance documents, reports and orders; and
- Other relevant briefing notes and other communications.

Interviews were conducted with management and staff from the OCIO's Privacy and Legislation Branch. OIPC examiners interviewed the eight individuals one-on-one for approximately one hour during March of 2014.

The interview guide included questions on:

- The goals and objectives of the Branch;
- Reporting relationships;
- Notifications to affected individuals;
- Reporting to the OIPC;
- Job duties and training;
- Breach investigations processes;
- Staffing, workload and internal procedures;
- File tracking; and
- Opportunities and challenges for breach management in BC Government.

File Review

This portion of the examination included analysis and reporting of overall statistics on information incidents; privacy breaches; and the sample of each selected for further review. A sample of OCIO investigative files were inspected in relation to the OIPC's recommended steps for responding to privacy breaches (containment, risk evaluation, notification, and prevention strategies); the responsibilities set out in FIPPA; and relevant BC Government policies and procedures.

Using standard statistical methods, the OIPC examination team selected a sample of 327 closed OCIO investigative files from 2012 and 2013 for review. This size of sample provides a five percentage point margin of error at a 95% confidence level, meaning that the sample selected for review will provide an accurate representation of the overall population of suspected privacy breaches in OCIO files from 2012 and 2013, give or take five percent, 19 times out of 20. A comparison of key demographics between the sample and the population of closed files from 2012 and 2013 shows that the sample mirrors the overall population on key characteristics such as year, ministry, and category of privacy breach. See Table 4 for detail.

Table 4: Comparison of Sample of Closed Investigations to Population of Suspected Privacy Breaches from 2012 to 2013

	Sample of Closed Privacy Breach Investigations		**Population of Suspected Privacy Breaches 2012-2013**	
Year	**#**	**%**	**#**	**%**
2012	163	49.8%	1105	49.6%
2013	164	50.2%	1123	50.4%
Ministry				
Health	86	26.3%	583	26.2%
Social Development and Social Innovation	85	26.0%	573	25.7%
Children and Family Development	51	15.6%	353	15.8%
Justice	42	12.8%	287	12.9%
BC Public Service Agency	17	5.2%	115	5.2%
Technology, Innovation and Citizens' Services	16	4.9%	110	4.9%
Finance	9	2.8%	60	2.7%
Energy and Mines	4	1.2%	29	1.3%
Forests, Lands and Natural Resource Operations	3	0.9%	23	1.0%
Jobs, Tourism and Skills Training	3	0.9%	21	0.9%
Advanced Education	3	0.9%	18	0.8%
Education	2	0.6%	16	0.7%
Other[70]	6	1.8%	40	1.8%
Category				
Administrative error	220	67.3%	1481	66.5%
Disclosure	56	17.1%	409	18.4%
Protection	11	3.4%	89	4.0%
Lost	13	4.0%	87	3.9%
Access	12	3.7%	78	3.5%
Stolen	5	1.5%	36	1.6%
Other	5	1.5%	18	0.8%
Collection	3	0.9%	15	0.7%
Cyber-attack	2	0.6%	10	0.4%
Use	0	0%	5	0.2%
Grand Total	**327**	**100%**	**2228**	**100%**

Ministry Processes Review

Information and findings related to the ministries' processes were based on a review of relevant ministry-specific policies and procedures relating to privacy; guidelines for contractors and service providers; relevant briefing notes and other communications; and interviews with key information and security staff from each of the ministries. Findings from the Ministry Process Review comprised an evaluation of ministry policies and practices within four key government ministries:

- Social Development and Social Innovation ("SDSI");
- Children and Family Development ("MCFD");
- Health ("MoH"); and
- Justice ("JAG").

The OIPC examination team selected these ministries based on a combination of the number of reported suspected information incidents and the sensitivity of personal information held by the ministry.[71]

Examiners interviewed Ministry Chief Information Officers, Ministry Information Security Officers, and others tasked with privacy and/or security functions during May of 2014 and included questions addressing the following topics:

- Roles and responsibilities;
- Privacy breach reporting;
- Safeguards and training;
- Personal information inventories;
- Service providers;
- Notifications to individuals;
- Reporting to the OCIO;
- Reporting to the OIPC;
- Privacy breach investigative processes;
- Analysis of breach files; and
- Opportunities and challenges for breach management in BC Government.

9.2 Appendix B: PIU Privacy Incident Category Definitions

1. (Access) Inappropriate access to personal information

Where an employee has accessed personal information stored in paper records or on a government information system (e.g. CORNET).

2. Administrative Error

This category includes incidents that are minor in nature and involve errors as a result of the inappropriate handling of government correspondence (e.g. email, mail, faxes, and physical documents that are inadvertently issued to an inappropriate recipient), and telephone transactions involving improper steps to identify a client.

When an incident is coded into this category it is also to be assigned to one of the following sub-categories:

- **Account error**
  Where a program area inadvertently updates the wrong account holder's information (*i.e.*, to add a dependent to an account, to change an address, etc.), but the error is discovered without any correspondence (in any form) being issued.
- **Bad Address**
  Includes incidents where an individual moves, but does not update their address held by government, which results in correspondence being issued to the incorrect location.
- **Email**
  Where an email containing personal information is sent to an unauthorized person. This includes government employees receiving emails intended for another government employee who has a very similar name.
- **Fax**
  Where a fax containing personal information is sent to an unauthorized person.
- **In-person**
  Where personal information is physically handed to an unauthorized person during a client interaction. This includes cheques and other documents being issued to the incorrect individual.

- **Mail**
  Where paper-based correspondence sent by traditional mail or courier is sent to, or received by, an unauthorized person. This includes "double-stuffed" envelopes, lost mail, and other incidents where mail is the mechanism by which the records are transited.
- **Other**
  Administrative/processing errors that do not fit into one of the other sub-categories.
- **Telephone**
  Administrative errors related to improper identification or verification of a client.

3. (Collection) Inappropriate collection of personal information

Where government inappropriately collects personal information from an individual (e.g. without consent or without a proper collection authority).

4. Cyber-attack

This includes incidents of malicious code (e.g. automated virus), hacking or phishing which result in a breach of personal information. These incidents are typically waged by non-B.C. government actors.

5. (Disclosure) Inappropriate disclosure of personal information

Includes verbal and other disclosures (e.g. improperly/unredacted files related to a court proceeding) of personal information to individuals not authorized to receive it.

6. Fraud

Where an individual who, by deceit, falsehood, or other fraudulent means:

(1) attempts to defraud any individual, organization, or public body of any property, money, or valuable security or any service;

or

(2) impersonates, or attempts to impersonate, another individual either living or dead

(i) with intent to gain advantage for themselves or another person;

(ii) with intent to obtain any property or an interest in any property;

(iii) with intent to cause disadvantage to the person being personated or another person; or

(iv) with intent to avoid arrest, prosecution, or another sanction that might be incurred as a result of their actions.

7. **Lost**

   Incidents involving a loss of government records containing personal information. This includes losses of paper records and electronic records stored on a technology device (cellular telephone, computer, thumb drive or other portable storage device) that was unencrypted (e.g. personal device) and/or insecure (e.g. password taped to side).

8. **Other**

   This category includes incidents that do not fall into any of the above categories.

9. **(Protection) Inadequate protection of personal information**

   Incidents where there has been no apparent disclosure or exchange of personal information, but there is a situation where a public body has not ensured that reasonable security measures are in place to protect personal information.

10. **(Stolen) Stolen asset - includes paper records**

    Incidents involving a theft of government records containing personal information. This includes thefts of paper records and electronic records stored on a technology device (cellular telephone, computer, thumb drive or other portable storage device) that was unencrypted (e.g. personal device) and/or insecure (e.g. password taped to side).

11. **(Use) Inappropriate use of personal information**

    Where a government employee or unit makes an improper use of personal or business sensitive information.

9.3 Appendix C: Reporting to OIPC – Examples for the Interim Standard

The purpose of this document is to illustrate, through the use of examples, the interim standard for reporting breaches to the OIPC. These cases are not examples of whether to notify affected individuals.

Interim Standard

Report all suspected breaches to the OIPC if the suspected breach:

a) involves personal information; and

b) could reasonably be expected to cause harm to the individual and/or involves a large number of individuals.

Examples of Privacy Harms

This report does not contain an exhaustive list of all the possible categories or types of privacy harms that affect individuals as a result of a breach. However, the Centre for Information Policy Leadership, in its 2014 paper, *A Risk-based Approach to Privacy: Improving Effectiveness in Practice* categorizes privacy harms to individuals under the headings of "tangible damage to individuals" and "intangible distress to individuals". Examples of privacy harms under these headings are:

Tangible damage, normally physical or economic, includes:

- bodily harm;
- loss of liberty or freedom of movement;
- damage to earning power; and
- other significant damage to economic interests, for example arising from identity theft.

Intangible distress, assessed objectively, includes:

- detriment arising from monitoring or exposure of identity, characteristics, activity, associations or opinions;
- chilling effect on freedom of speech, association, etc.;
- reputational harm;
- personal, family, workplace or social fear, embarrassment, apprehension or anxiety;
- unacceptable intrusion into private life; and
- discrimination or stigmatisation.[72]

These concepts are used in the examples that follow to describe whether there exists a reasonable expectation of harm to individuals.

Example 1: Stolen Briefcase

An employee's briefcase is stolen from a vehicle. The briefcase contains paper files relating to three individuals and a laptop that contains personal information of ten individuals. The laptop is encrypted.

The personal information contained on the laptop and in the paper files includes name, address, telephone number, personal health number and diagnosis.

Neither the laptop nor the paper files are recovered.

Does the breach involve a large number of individuals?

No

Could this breach reasonably be expected to cause harm to the individuals?

A properly encrypted laptop is considered sufficient protection from unauthorized access. While the laptop was not recovered, one would not reasonably expect the individuals to be caused harm because the personal information on the device was, with encryption, sufficiently safeguarded from unauthorized access.

The (unencrypted) personal information in the paper files was left in a vehicle and was therefore not sufficiently safeguarded. It is sensitive personal information (diagnosis) that if disclosed could cause embarrassment, apprehension or anxiety and personal information (name, address, telephone number) that could cause damage to economic interests, for example arising from identity theft.

As the information has not been recovered – and unless it was recovered almost immediately – there remains a reasonable expectation that affected individuals could be caused harm by the breach of the personal information in the paper files.

Should this breach be reported to the OIPC?

Yes

What does the example illuminate or clarify?

- Proper encryption reasonably protects personal information from unauthorized access, use, or disclosure,
- If the breached personal information is encrypted, it may not be necessary to report the breach to the OIPC.

Example 2: Misplaced File

After a move between offices, it is discovered that a report related to an inquiry into the death of a youth is missing. The report includes mental health assessments and other documents about the youth and the youth's parents.

The report is not recovered but there is no evidence to suggest that the personal information is being inappropriately used. In other words, there remains a chance that the report has simply been misfiled and is not actually in the hands of unauthorized persons.

Does the breach involve a large number of individuals?

No

Could this breach reasonably be expected to cause harm to the individuals?

The personal information is highly sensitive (mental health assessments, etc.). If the personal information is in the hands of unauthorized individuals, it is reasonable to expect that the parents would be caused personal, family, workplace or social fear, embarrassment, apprehension or anxiety; and unacceptable intrusion into private life.

While the likelihood of the harm occurring appears to be low because there is no evidence of inappropriate use; the lack of containment, along with the sensitivity of the personal information, means that there remains a reasonable expectation that harm could result.

Should this breach be reported to the OIPC?

Yes

What does the example illuminate or clarify?

- Lack of containment – or the inability to confirm that the personal information is protected – leaves the personal information vulnerable.
- If harm is still reasonably expected to occur, report the breach to the OIPC.

Example 3: Accessible Employee Files

Twenty-five government employee files were accessible by all employees as they were inappropriately, but temporarily, located on a shared drive. The personal information includes name, home address, telephone numbers, email address, SIN, gender, emergency contacts, leave and benefit information, T4 information and pay cheque information.

The matter is rectified as soon as the problem is discovered by restoring the appropriate role-based permissions on the shared drive.

Later that day, because the employer has audit capabilities, the employer is able to determine that no files were actually accessed by any employee except the government employee who discovered and reported the breach. It is confirmed that this employee spent less than two minutes at the shared drive location and the employee is willing to provide written confirmation that no information was printed or otherwise used or transmitted. In addition, the government employee has already signed an oath of employment, which includes agreeing to safeguard confidential information.

Does the breach involve a large number of individuals?

No

Could this breach reasonably be expected to cause harm to the individuals?

A breach will not generally be expected to cause damage to economic interests arising from identity theft; or reputational harm or embarrassment, apprehension or anxiety) when it has been confirmed that no files were actually accessed other than by the reporting employee in the circumstances described above.

Should this breach be reported to the OIPC?

No, unless assistance with respect to breach management is sought.

Note: If the employer was unable to confirm in a timely fashion that files had not been accessed, there would be a reasonable expectation that harm would be caused and the breach should be reported to the OIPC.

What does the example illuminate or clarify?

- Appropriate and timely containment can reduce the possibility that harm would be caused; and
- Accidental inappropriate access (if contained) may not have to be reported.

Example 4: Group Email

A public body sends a group email to ten participants advising of a change of venue for a presentation on applying the provincial sales tax for which the individuals had previously registered. The email is sent without using the 'undisclosed recipient' function, thereby disclosing personal information of the individuals (email addresses, some names and the fact that these individuals had registered for the provincial sales tax presentation).

Does the breach involve a large number of individuals?

No

Could this breach reasonably be expected to cause harm to the individuals?

Generally, on their own, names and email addresses are not considered sensitive personal information, nor is the application of the provincial sales tax a particularly sensitive program. It is therefore unlikely that the disclosure of this information could reasonably be expected to cause harm to the individuals.

Should this breach be reported to the OIPC?

No

Note: If the group email had been sent to 500 individuals, the incident should be reported to the OIPC based on it involving a large number of individuals, regardless that it is not reasonably expected to cause injury or harm to the individuals.

What does the example illuminate or clarify?

- Breaches that are unlikely to cause harm to the individuals do not necessarily need to be reported to the OIPC; and
- Large numbers of individuals must be reported regardless of harm.

Example 5: Inappropriate Access

An employee of a public body accesses a workplace database that contains medical information of thousands of individuals. The employee has a legitimate work reason for accessing the database generally but is only authorized to access the medical information of individuals for work related reasons.

The employee accesses the medical information of a former partner. The access is not work related. The employer has a strict policy that prohibits employees from accessing the medical information of any individual for non-work related purposes.

The employee confirms in writing that they have not and will not use or disclose the personal information. The employer ensures that the employee is reminded of and understands their privacy obligations and will refresh their privacy training.

Does the breach involve a large number of individuals?

No

Could this breach reasonably be expected to cause harm to the individuals?

Whether or not the employee used or disclosed the personal information of the former partner, the fact that the employee accessed the personal information and could, at any time in the future, use or disclose the information – regardless of the written declaration – means that there remains a reasonable expectation that the access could cause harm (*e.g.,* reputational harm; embarrassment, apprehension or anxiety; unacceptable intrusion into private life).

Should this breach be reported to the OIPC?

Yes

What does the example illuminate or clarify?

- Regardless of the intent of the individual or any written declaration, intentional inappropriate access (*i.e.,* snooping) should always be reported to the OIPC.

Endnotes

[1] Office of the Information and Privacy Commissioner, 2012, *Privacy Breaches: Tools and Resources*, p. 3, (www.oipc.bc.ca/guidance-documents/1428).
[2] Office of the Information and Privacy Commissioner, *Accountable Privacy Management in BC's Public Sector*, pp. 14-15 (www.oipc.bc.ca/guidance-documents/1545).
[3] Office of the Information and Privacy Commissioner, Investigation Report F06-02, para. 81, (www.oipc.bc.ca/investigation-reports/1233).
[4] Office of the Information and Privacy Commissioner, Investigation Report F13-02, section 2.2, p. 20 (www.oipc.bc.ca/investigation-reports/1546).
[5] Office of the Information and Privacy Commissioner, Investigation Report F06-02, para. 55, (www.oipc.bc.ca/investigation-reports/1233).
[6] Office of the Information and Privacy Commissioner, Investigation Report F08-02; p. 12, (www.oipc.bc.ca/investigation-reports/1236).
[7] Office of the Information and Privacy Commissioner, *Accountable Privacy Management in BC's Public Sector*, pp. 14-15 (www.oipc.bc.ca/guidance-documents/1545); Office of the Information and Privacy Commissioner, 2012, *Privacy Breaches: Tools and Resources*, pp. 7-9, (www.oipc.bc.ca/guidance-documents/1428).
[8] *Freedom of Information and Protection of Privacy Act*, [RSBC 1996] CHAPTER 165, Schedule 1 (Definitions), (www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/96165_00).
[9] Ministry of Technology, Innovation and Citizens' Services, Office of the Chief Information Officer, Governance,(www.cio.gov.bc.ca/cio/about/governance/governance.page).
[10] Office of the Chief Information Officer, (www.cio.gov.bc.ca/cio/priv_leg/index.page).
[11] BC Government Core Policy and Procedures Manual (Core Policy), Chapter 12.2.2 (IM/IT Governance), (www.fin.gov.bc.ca/ocg/fmb/manuals/CPM/12_Info_Mgmt_and_Info_Tech.htm).
[12] Ministry of Citizens' Services, Office of the Chief Information Officer, January 29, 2010, *Internal Review – Privacy Breach Ministries of Housing and Social Development & Children and Family Development*; pp. 15-16.
[13] Ministry of Technology, Innovation and Citizens' Services, *2012/2013 Annual Report on the Administration of the Freedom of Information and Protection of Privacy Act*, p. 10.
[14] The Personal Information Directory is a list of summaries of privacy impact assessments, ministries personal information banks, health information banks, and information sharing agreements for all government.
[15] The PIU, for the purposes of this examination report, is meant to comprise all staff across the branch who conduct privacy investigations, regardless of from which work unit the staff originates.
[16] Office of the Information and Privacy Commissioner. Investigation Report F13-02, section 3.0, pp. 25-26, (www.oipc.bc.ca/investigation-reports/1546).
[17] BC Government Core Policy, Chapters 12.3.6, 15.2, 20, L and OCIO *Information Incident Management Process* (IIMP), (www.cio.gov.bc.ca/cio/information_incident/index.page).
[18] *Information Incident Management Process*, section 1, p. 5, (www.cio.gov.bc.ca/cio/information_incident/index.page).
[19] *Information Incident Management Process*, section 1, p. 5, (www.cio.gov.bc.ca/cio/information_incident/index.page).
[20] BC Government, *Process for Responding to Privacy Breaches*, p. 7, (www.cio.gov.bc.ca/cio/information_incident/index.page).
[21] Ministry of Social Development and Social Innovation, 2011, *FOIPPA Access to Information and Protection of Privacy Policy* and *Information Security Guidelines for Service Providers*.
[22] Ministry for Children and Family Development, Information Briefing Note (CLIFF#217460), p. 3.
[23] Ministry for Children and Family Development, Information Briefing Note (CLIFF#217460), pp. 3-4.

[24] The BC Government, *General Services Agreement, Schedule E*, Section 12 requires that the contractor make reasonable security arrangements to protect personal information. Section 19 requires that contracts immediately notify the Province of any unauthorized disclosure of personal information, as per Section 30.5 of FIPPA, (http://www.pss.gov.bc.ca/psb/gsa/docs/GSA_May_14_2014.docx).

[25] Ministry for Children and Family Development, *Contractor's Records Guidelines,* p. 1*,* (www.mcf.gov.bc.ca/service_providers/pdf/contractor_records_guidelines.pdf).

[26] Ministry for Children and Family Development, *Contractor's Records Guidelines*, p. 1, (www.mcf.gov.bc.ca/service_providers/pdf/contractor_records_guidelines.pdf).

[27] Ministry of Health, *Information Privacy Policy*, p. 1.

[28] Ministry of Health, *Information Privacy Policy*, p. 9.

[29] Ministry of Justice, May 2, 2014 Email, copy provided to OIPC.

[30] Ministry of Justice, BC Corrections Branch, *Management Services Policy Manual*, Chapter 2.4 Information Incidents.

[31] Office of the Information and Privacy Commissioner, Investigation Report F13-02, Section 3.0, pp. 25-26.

[32] The PIU Management include, for the purposes of this examination report, the Executive Director of the Branch and the Director of the PIU.

[33] *Information Incident Management Process*, p. 8, (www.cio.gov.bc.ca/cio/information_incident/index.page).

[34] *Information Incident Management Process*, pp 8, (www.cio.gov.bc.ca/cio/information_incident/index.page).

[35] *Information Incident Management Process*, p. 9, (www.cio.gov.bc.ca/cio/information_incident/index.page).

[36] *Information Incident Management Process*, pp 9-10, (www.cio.gov.bc.ca/cio/information_incident/index.page).

[37] Ministry of Citizens' Services, Office of the Chief Information Officer, January 29, 2010, *Internal Review – Privacy Breach Ministries of Housing and Social Development & Children and Family Development,* p.16*.*

[38] Ministry of Technology, Innovation and Citizens' Services, *2012/2013 Annual Report on the Administration of the Freedom of Information and Protection of Privacy Act*, p. 12.

[39] BC Government, *IM111-Information Sharing and Privacy Awareness Training for Employees.*

[40] BC Government, *IM111-Information Sharing and Privacy Awareness Training for Employees*.

[41] Office of the Chief Information Officer, August 19, 2014 Email sent to the Office of the Information and Privacy Commissioner.

[42] Office of the Chief Information Officer, June 4, 2014 Email sent to the Office of the Information and Privacy Commissioner.

[43] 2010 numbers reflect a 9 (not 12) month period.

[44] As these numbers are based on calendar year and not fiscal year, they do not match those reflected in the Ministry of Technology, Innovation and Citizens' Services' *2012/2013 Annual Report on the Administration of FIPPA*.

[45] Office of the Chief Information Officer, October 1, 2013. PRIU privacy incident categories, p.1.

[46] "Other" includes Ministries of Agriculture, Community, Sport and Cultural Development, Natural Gas Development, Aboriginal Relations and Reconciliation, Transportation and Infrastructure and Environment, and other BC Government agencies categorized as "other" in the population dataset.

[47] Office of the Information and Privacy Commissioner, *Accountable Privacy Management in BC's Public Sector*, p. 6, (www.oipc.bc.ca/guidance-documents/1545).

[48] BC Government, *Core Policy and Procedures Manual*, Section 12.3.6, Policy b(2). Office of the Chief Information Officer, *September 2011, Information Incident Management Process,* Section 1, Policy 2. BC Government, *Process for Responding to Privacy Breaches*, (www.cio.gov.bc.ca/cio/information_incident/index.page).

[49] Office of the Information and Privacy Commissioner, 2012, *Privacy Breaches: Tools and Resources*, p. 18, (www.oipc.bc.ca/guidance-documents/1428).

[50] BC Government, *Process for Responding to Privacy Breaches,* pp. 2-3, (www.cio.gov.bc.ca/cio/information_incident/index.page).

[51] Centre for Information Policy Leadership, 2014, *The Role of Risk Management in Data Protection,* p. 17, (http://www.informationpolicycentre.com/files/Uploads/Documents/Centre/The_Role_of_Risk_Management_in_Data_Protection_FINAL_Paper.PDF).

[52] Statistical data is not provided because the *Information Incident Report Form* was not always submitted to the OCIO and, if submitted, the harms section was not consistently completed.

[53] OIPC examiners acknowledge that some of these files may indeed be of low risk. One example of this is with regard to HIBC files; however, OIPC examiners were advised that HIBC breach reporting processes have changed since the examination was conducted.

[54] Office of the Information and Privacy Commissioner, 2012, *Privacy Breaches: Tools and Resources*, p. 18, (www.oipc.bc.ca/guidance-documents/1428).

[55] Investigation Report F08-02, p. 12, (www.oipc.bc.ca/investigation-reports/1236).

[56] BC Government, *Process for Responding to Privacy Breaches*, p. 4, (www.cio.gov.bc.ca/cio/information_incident/index.page).

[57] Office of the Chief Information Officer, *September 2011, Information Incident Management Process,* p. 9, (www.cio.gov.bc.ca/cio/information_incident/index.page).

[58] Office of the Information and Privacy Commissioner, 2012, *Privacy Breaches: Tools and Resources*, p. 8, (www.oipc.bc.ca/guidance-documents/1428); BC Government, *Process for Responding to Privacy Breaches*, p. 4, (www.cio.gov.bc.ca/cio/information_incident/index.page).

[59] Office of the Information and Privacy Commissioner, *Accountable Privacy Management in BC's Public Sector*, pp. 14-15, (www.oipc.bc.ca/guidance-documents/1545); Investigation Report F08-02, p. 10.

[60] Office of the Information and Privacy Commissioner, 2012, *Privacy Breaches: Tools and Resources*, p. 18, (www.oipc.bc.ca/guidance-documents/1428).

[61] Treasury Board of Canada Secretariat, 2014, *Guidelines for Privacy Breaches, (*http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=26154&section=text), Section 4.

[62] Office of the Information and Privacy Commissioner, 2012, *Privacy Breaches: Tools and Resources,* p. 10, (www.oipc.bc.ca/guidance-documents/1428).

[63] 227 files of the 250 actual breaches contained in the sample.

[64] There did not appear to be any substantive difference between the OCIO prevention categories of practice/procedure and business process so these two fields were grouped together for analysis.

[65] Office of the Information and Privacy Commissioner, 2012, *Privacy Breaches: Tools and Resources*, p. 10, (www.oipc.bc.ca/guidance-documents/1428); Office of the Information and Privacy Commissioner, *Accountable Privacy Management in BC's Public Sector*, p. 14, (www.oipc.bc.ca/guidance-documents/1545).

[66] Office of the Information and Privacy Commissioner, *Accountable Privacy Management in BC's Public Sector*, pp. 14-15, (www.oipc.bc.ca/guidance-documents/1545).

[67] Office of the Information and Privacy Commissioner, *Accountable Privacy Management in BC's Public Sector*, pp. 14-15, (www.oipc.bc.ca/guidance-documents/1545); Office of the Information and Privacy Commissioner, Investigation Report F06-02, para. 55, (www.oipc.bc.ca/investigation-reports/1233).

[68] Office of the Information and Privacy Commissioner, *Accountable Privacy Management in BC's Public Sector*, pp. 14-15, (www.oipc.bc.ca/guidance-documents/1545).

[69] Office of the Information and Privacy Commissioner, *Accountable Privacy Management in BC's Public Sector*, p. 13, (www.oipc.bc.ca/guidance-documents/1545).

[70] Other includes Ministries of Agriculture, Community, Sport and Cultural Development, Natural Gas Development, Aboriginal Relations and Reconciliation, Transportation and Infrastructure and Environment, the Office of the Premier, and other BC Government agencies categorized as "other" in the original population dataset.

[71] Office of the Information and Privacy Commissioner, Investigation Report F13-02, Section 3.0, p. 5, (www.oipc.bc.ca/investigation-reports/1546).

[72] Centre for Information Policy Leadership, 2014, *The Role of Risk Management in Data Protection*, p.17. (http://www.informationpolicycentre.com/files/Uploads/Documents/Centre/The_Role_of_Risk_Management_in_Data_Protection_FINAL_Paper.PDF).