Improving the measurement of digital security incidents (Privacy authority perspectives): Taking stock and priorities for action

RESULTS OF A SURVEY OF STATISTICAL PRACTICES OF SELECTED PRIVACY AUTHORITIES IN RELATION TO BREACH NOTIFICATION

18 April 2017

Survey and report author: Blair Stewart, Office of the Privacy Commissioner, New Zealand

Undertaken with the cooperation of the:

- ICDPPC Data Protection Metrics Working Group
- APPA Comparative Privacy Statistics Working Group

RESULTS OF A SURVEY OF STATISTICAL PRACTICES OF SELECTED PRIVACY AUTHORITIES IN RELATION TO BREACH NOTIFICATION

Report by Blair Stewart, New Zealand, 18 April 2017

Summary

The survey explores the statistical practices of several privacy authorities that currently receive self-reported notification of breaches. The survey asked how statistics relating to notified breaches are kept, used and disseminated. It was found that while some authorities produce separate breach notification statistics the source of the information is generally kept within systems maintained for handling complaints and investigations. The statistics fell into 3 categories: the report/breach; the reporting entity; processing by the authority. The 4 uses of the statistics were to: Aid understanding of problems; public advocacy; to guide authority action, to assess regulatory effectiveness.

Responses

On 23 and 24 March 2017 a link to a short online survey (attachment 1) was separately sent to the members of both the ICDPPC Data Protection Metrics Working Group and of the APPA Comparative Privacy Statistics Working Group. The survey sought information privacy breach notification statistics gathered, used or disseminated by privacy and data protection authorities.

Responses were received between 24 March and 13 April 2017 with several additional partial responses in some cases advising that they had no applicable breach notification scheme. This report draws upon responses from 8 authorities based in Australia, Canada, Greece, Korea, Latvia, Mauritius, Ontario, New Zealand and the UK that advised that they received breach notifications.

Part A: Existing breach notification metrics

Questions regarding internal statistics kept and their use

Do you currently maintain an internal statistical database of the breaches notified to your authority?

6 authorities maintained internal statistical databases of the breaches notified to them

In answer to the question 'how do you keep those statistics and what are they used for?' and 'what measures/statistics do you keep?' respondents advised:

Respondent authority	How statistics are kept and their use	List of measures/statistics
Australia, Office of the Australian Information Commissioner	Although not a dedicated statistical database, the OAIC's case management system can be used to build various statistical reports.	The main measures we report on are number of notifications received and number of notifications by industry sector From next financial year we will also be reporting on categories of breach (malicious or criminal act; system glitch; human error) and size of breach (number of people affected).
Canada, Office of the Privacy Commissioner of Canada	These statistics are kept on our Office's electronic records management system. The statistical data elements are used for: • Annual Reporting purposes: • For appearances before Parliament to inform Parliamentarians • Compliance activities • Developing policy positions • Identifying trends for informing education and outreach activities • Informing audits that our Office may undertake • For speeches before industry groups or government office holders. NOTE: The May 2014 Directive on Privacy Practices requires federal government institutions to report all privacy breaches that could reasonably be expected to cause serious injury or harm to the individual to the Privacy Commissioner of Canada and to the Treasury Board of Canada Secretariat. For organizations that are subject to Canada's federal private sector privacy legislation breach reporting is currently voluntary. Legislation has been passed for mandatory breach reporting, but it has not come into force. It is expected to come into force when the associated regulations are passed. When that happens, those organizations will be required to report breaches that represent a real risk of significant harm to individuals to the Privacy Commissioner of Canada. In Canada there are also Data Protection Authorities (DPAs) at the provincial and territorial level. For provincial and territorial government department and agencies, they would have obligations in law to report to their respective provincial and territorial DPAs. As well, certain provinces have also established health privacy and general privacy legislation that may have data breach reporting obligations.	For statistics related to federal government institutions, breaches are recorded by name of the organization, and for statistics related to organizations subject to federal private-sector privacy legislation, breaches are recorded by sector. In both instances the incident type and total incidents per year are also recorded. Reports of public sector breaches include the nature and extent of the breach; the type of personal information involved; the parties involved; steps taken or to be taken to notify individuals; and what remedial action has been taken. For private sector breaches, we also capture number of total individuals affected, number of Canadians affected, dates of occurrence and detection, who notified us of the breach, whether affected individuals were notified, and industry sector.
Greece, Hellenic Data Protection Authority	This respondent advised that no internal statistical database was maintained. An explanation was added to the effect that the only notification obligation concerned electronic communications (under Directive (EC) 2002/58) and "The number of data breach incidents notified is very small, a few incidents every year."	-

Korea, Korea Internet & Security Agency (KISA)	We are notified frequently through the website related to personal data breaches and are automatically stored in DB. The websites are: • https://www.i-privacy.kr (funded by KCC [Korea Communications Commission], operated by KISA) • https://www.privacy.go.kr (funded by MoI [Ministry of Interior], operated by KISA) The statistical data are used only as basic data for the policy to prevent the secondary damage, and KISA do not publicly disclose the data.	KISA receive notification data as follows : • company's name, • reporting date, • item of the personal information leaked, • point of time the personal information is leaked, • number of the personal information leaked, • outline of the personal information leaked • date of investigation
Mauritius, Data Protection Office	To analyse trends To evaluate the office's success in sensitising data controllers and the public and also in enforcing data protection principles and help to implement corrective measures	Number of complaints lodged at the office Number of decisions given by the Commissioner following the completion of investigations on the complaints Number of complaints referred to the police for prosecution
New Zealand, Office of the Privacy Commissioner	Statistical reporting. Threat pattern identification. Public education	• Number of breaches reported • Organisation (or individual) • Date breach reported • Date breach occurred (where known) • Date breach identified (where known) • Contact person details • Type of organisation (sector) • Type of breach • Following OPC published guidelines for handling breach? • Number of people affected (if known) • Details of how breach occurred • Details of steps taken to remediate • Details of advice given • Name of person in OPC giving advice
Ontario, Office of the Information and Privacy Commissioner	The statistics are generated from privacy complaint files that are kept in our internal case management system. The statistics are used for public education and advocacy as well as to provide a review of the effectiveness of Ontario's privacy laws in our annual report.	Our office keeps statistics on the general metric of "privacy complaints" with respect to the following measures: • Total number closed • Closed by type of resolution (resolved, screened out, withdrawn, abandoned, report) • Source of complaint (individual, IPC Commissioner initiated, self-reported breach) • Type of resolution (resolved, screened out, withdrawn, abandoned, report) and stage closed (intake, investigation) • Issues (disclosure, security, collection, general privacy issue, use, access, inappropriate access, disposal, personal information) • Outcome of issues (resolved – finding not necessary, complied in full, Act does not apply, complied in part) • Processed in intake by disposition (resolved, screened out without subs, withdrawn, proceed to investigation, abandoned) • Processed by investigation by disposition (report, resolved)
UK, Information Commissioner's Office	All self-reported breaches are entered into a central case management system. Data controllers can report the breaches using an online tool available on the ICO website: https://ico.org.uk/for-organisations/report-a-breach/ The form is divided up in 7 sections. The responses provided by the data controller help ascertain the extent to which they are deemed to have complied with Principle 7 of the Data Protection Act 1998 (DPA).	• Organisation details (name, registration number, primary contact details) • Details of the data protection breach (date, circumstances, delay in reporting, measures in place to prevent this type of incidents, details of policies and procedures) • Personal data placed at risk (type of data, number of individuals affected, of victims' awareness, possible risks, complaints received in relation to the incident)

	Under Principle 7 of the DPA, data controllers must adopt "appropriate technical and organisational measures […] against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data" and "having regard to the state of technological development and the cost of implementing any measures, the measures must ensure a level of security appropriate to (a) the harm that might result from such unauthorised or unlawful processing or accidental loss, destruction or damage as are mentioned in the seventh principle, and (b) the nature of the data to be protected. The information reported by data controllers is then copied on an Excel spreadsheet which is used to assess the nature of the infringement as well as the harm which has resulted or is likely to result from the infringement. ICO maintains the database, from which statistics can be drawn. This system is not publicly accessible.	• Containment and recovery (actions taken by the data controller, data recovered, new preventive measures) • Training and guidance (type, nature and frequency of training, staff guidance on the handling of personal data) • Previous contact with the ICO (other recent incidents) • Miscellaneous (notification of other DPAs, of the Police or of other regulatory authorities)

Comment by author: How statistics are kept

Not all respondents provided information on 'how' statistics are kept but it appears that separate systems have generally not been created for breach notification statistics. Instead, in at least some authorities breach notification records have found a place within existing administrative systems for 'cases' or 'complaints'. This is understandable in that a complaints body may treat notifications as simply one source of subject matter to be processed through statutory systems laid out for dispute resolution or compliance action. ("If all you have is a hammer, everything looks like a nail.") There are some conceptual and administrative challenges to treating self-reporting as equivalent to lodging a complaint and this may colour some of the statistics generated and used.

Interestingly, several authorities (e.g. UK ICO) solicit notifications with online templates which are well suited to building standardised statistical data sets as well as achieving their primary purposes.

Comment by author: Statistics kept

The statistics kept generally fall into 3 categories:
1. The report and breach (numbers, type of breach, dates, size, etc.).
2. The reporter (e.g. industry or sector).
3. Processing (actions taken, entry into statutory channels such as formal complaint, outcomes, whether guidelines have been followed, etc.).

It is not always clear that the responses to the question have confined themselves to statistical records. As mentioned already, many authorities may integrate notifications into existing administrative processes and records systems and thus may, for instance, see notifications as simply an entry into a complaints channel. It is possible that some of the 'processing-type' categories of information listed above may be narrative information (e.g. about the perceived risk or the remedial action has been taken) rather than statistics alone.

One response suggests an evolution of statistical practice with experience ("From next financial year we will also be reporting on categories of breach (malicious or criminal act; system glitch; human error) and size of breach (number of people affected)."). Another notes changes will result from a forthcoming transition from a voluntary to mandatory system.

Comment by author: Use of statistics

The uses of the statistics might be placed in 4 groups:

1. Aid understanding of data protection problems (‘to analyse trends’, ‘threat pattern identification’).
2. Use in public messaging (‘public education and advocacy’).
3. To guide privacy authority action (‘use in enforcing data protection principles’, ‘help to implement corrective measures’, ‘develop policy positions’, ‘inform audits’).
4. To help assess effectiveness of law or privacy authority’s actions (‘to evaluate the office’s success in sensitising data controllers and the public’, ‘to provide a review of the effectiveness of privacy laws’).

The short survey did not seek any evidence of such uses. Seeking practical examples in future research might give a better picture of the reality of the use of the statistics and which measures are more useful for the most important purposes.

Questions regarding external reporting

Do you make any reports outside your authority that draw upon statistics of the breaches notified to your authority?

7 authorities reported that they made external statistical reports.

In answer to the question ‘to whom do you report and how often?’, ‘what measures/statistics are included?’ and ‘do these reports get made public and if so are they online?’ respondents advised:

Respondent authority	Reports addressed to/frequency	measures/statistics	Public/URL
Australia, Office of the Australian Information Commissioner	The OAIC annually publishes some DBN statistics in its annual report.	Number of notifications; breaches by sector.	Annual report: https://www.oaic.gov.au/about-us/corporate-information/annual-reports/all/ Performance portal: https://www.oaic.gov.au/performance
Canada, Office of the Privacy Commissioner of Canada	We report on breaches to inform discussions at international fora including APPA (Asia Pacific Privacy Authorities). APPA reporting is twice/year	For statistics related to federal government institutions, breaches are recorded by name of the organization, and for statistics related to organizations subject to federal private-sector privacy legislation, breaches are recorded by sector. In both instances the incident type and total incidents per year are also recorded. For APPA mostly aggregate figures (public and private sector)	Our Office’s Annual Reports to Parliament can be found via this link: https://www.priv.gc.ca/en/opc-actions-and-decisions/reports-to-parliament/ Please note: Within Canada, Provincial and Territorial DPAs also maintain statistics related to breaches, which can be found in their respective Annual Reports. Links to all of these DPA’s Annual Reports can be found via this link: https://www.priv.gc.ca/en/about-the-opc/what-we-do/provincial-and-territorial-collaboration/provincial-and-territorial-privacy-laws-and-oversight/
Greece, Hellenic Data Protection Authority	DPA's annual report includes statistics and is addressed to the Parliament, public authorities &. However, as to data breach notifications, due to their small number, they are not presented as statistics but are described in the corresponding section of the report.	-	Annual reports are online, but only in Greek: http://www.dpa.gr/portal/page?_pageid=33,15078&_dad=portal&_schema=PORTAL
Mauritius, Data Protection Office	To our parent ministry, Ministry of Technology, Communication and Innovation On a quarterly basis but anonymised	Number of complaints lodged at the office Number of decisions given by Commissioner following completion of investigations of complaints Number of complaints referred to the police for prosecution	Yes. They are published on our website but anonymised: http://dataprotection.govmu.org/English/Pages/Decisions-on-Complaints.aspx
New Zealand, Office of the Privacy Commissioner	4 monthly to Minister of Justice Annually to Parliament Periodic website ‘snapshot’ reporting to public Reports to APPA Forum	To the minister: Number of breaches notified. Annually: Number of breaches, numbers of common types of breaches Snapshot: No of files by public/private sector	Annual report: https://privacy.org.nz/news-and-publications/corporate-reports/annual-report-of-the-privacy-commissioner-2016/ Snapshot reporting on OPC complaints, breach notifications and e-learning reporting: https://privacy.org.nz/about-us/transparency-and-accountability/complaints-breach-e-learning-reporting/

	as requested using a template, typically twice yearly	APPA Forum reporting template typically sought statistics on: • Total number • Number in public sector • Number in private sector • Number formally investigated • Number subject to media interest?	
Ontario, Office of the Information and Privacy Commissioner	Our office submits an annual report to the Legislative Assembly of Ontario (Ontario government).	Our office keeps statistics on the general metric of "privacy complaints" with respect to the following measures: • Total number closed • Closed by type of resolution • Source of complaint (including self-reported breach) • Type of resolution • Issues and Outcome of issues • Processed in intake by disposition • Processed by investigation by disposition	The reports are made public and are available online at: https://www.ipc.on.ca/about-us/annual-reports/
UK, Information Commissioner's Office	Annual report presented before Parliament Online trends report	CSV file: Type of incidents by sector (Loss/ theft of paperwork, Data posted/ faxed to incorrect recipient, Data sent by email to incorrect recipient, Insecure webpage (including hacking), Loss /theft of unencrypted device, Insecure disposal of paperwork, Failure to redact data, Information uploaded to webpage, Verbal disclosure, Insecure disposal of hardware, Other principle 7 failure)	CSV file https://ico.org.uk/media/action-weve-taken/2013831/data-security-incidents-csv.xlsx Data security incident trends https://ico.org.uk/action-weve-taken/data-security-incident-trends/

Drawn from the URLs given in the RH column, attachment 2 provides several illustrative samples of published breach notification statistics. In addition, an extract from an APPA Forum template (referenced in the Canadian and NZ responses) is displayed.

Comment by author: External reporting

The survey did not ask whether authorities publicly release notices received or identifiable details of reported breaches. Further research might usefully explore the purposes of and relationship between release of identifiable and statistical information on notified breaches.

The survey suggests that many privacy authorities periodically provide statistical reports on breach notification to the relevant governance bodies (typically a responsible government Minister and the legislature). Some may post periodic 'dashboard' type reports on their website.

Questions regarding central repository

The questionnaire asked about the existence of central repositories of breach notification statistics in the jurisdiction. The question was intended to tease out if there was a consolidated database to which more than one authority reported, an 'officially sanctioned' database or a public register of some kind. This question was not intended to replicate the questions about the authority's own internal records but was answered by most respondents as if it was. This may be due to the question being poorly worded or because there were no other known repositories. Accordingly, most answers given essentially replicate the earlier answers and so are not repeated here.

One exception was the response from the authority in Canada which advised:

> *The Treasury Board of Canada Secretariat also maintains data on breach notifications it receives from government institutions (this data is not made publicly available, but is reported on in aggregate for trend spotting).*
>
> *Our [OPC] repository is maintained internally by enforcement staff. The Treasury Board of Canada Secretariat (TBS) also maintains, internally, data on breach notifications it receives from government institutions.*
>
> *The OPC and TBS repositories include not just statistics but also full details of breach reports. Reasons include: a) complying with record keeping obligations, b) historical statistics generation for trend spotting (which can drive action such as press releases), c) used to identify and write case studies with educational value for website (include link to breach case summaries) d) for in cases of repeat breaches by the same organization, previous breach data is used to inform response to new breaches*

Although Korea's KISA response did not answer the questions about a central repository, its earlier answers did indicate that KISA was the destination for structured notifications received through two websites funded by two other government Ministries giving effect to two separate breach notification laws. In that sense the KISA database does have some characteristics of a central repository in the sense intended by the question.

However, the supplementary question seeking views on the purpose of maintaining a central repository did yield additional information albeit also referencing the authorities' own records. Answers included:

Respondent authority	In your opinion, why is the repository maintained
Australia, Office of the Australian Information Commissioner	To maintain records of reported breaches and OAIC response (required by the Australian Archives Act). To provide reporting functionality. To facilitate case management/investigation of breaches.
Canada, Office of the Privacy Commissioner of Canada	Complying with record keeping obligations Historical statistics generation for trend spotting (which can drive action such as press releases) Used to identify and write case studies with educational value for website (include link to breach case summaries) In cases of repeat breaches by the same organization, previous breach data is used to inform response to new breaches
Mauritius, Data Protection Office	To ensure the information available is accurate and up to date
New Zealand, Office of the Privacy Commissioner	Statistical reporting. Threat pattern identification. Public education
Ontario, Office of the Information and Privacy Commissioner	Our office is the custodian of the statistics, which are public. Our office's annual report must provide a comprehensive review of the effectiveness of Ontario's privacy laws, including: • an assessment of the extent to which institutions are complying with Ontario's

	privacy laws; and • the Commissioner’s recommendations with respect to the practices of particular institutions and with respect to proposed revisions to Ontario’s privacy laws.
UK, Information Commissioner’s Office	Maintaining statistics on the types of breaches and the sectors

Comment by author: Purposes of repositories of breach statistics

The question partly covers similar ground as the earlier question about use of the statistics produced. However, it might be taken to look beyond immediate short term use by the privacy authority to the reasons for a longer term collection of data. Suggested purposes fall generally into the following categories:

Archival responsibilities (which are given as a legal responsibility of privacy authorities but from which one can also infer the underlying purposes of records or archives laws such as government accountability, public confidence, national memory, etc.).

To directly support breach management (‘To facilitate case management/investigation of breaches’, to identify ‘cases of repeat breaches by the same organisation’).

To provide a broader or longer term view (‘historical statistics generation’, ‘trend spotting’, ‘threat pattern identification’).

The question did not seek practical examples of the suggested uses (such as ‘trend spotting’) nor did it ask about external access to the statistical database by researchers or other public bodies. These could be useful lines of future enquiry if the data sets are believed to have a longer term value.

Classification of breach types

Although the survey did not separately ask for a classification of breach types several responses, or linked reports, do offer a classification. These included:

Authority	Types of breaches
Australia, OAIC	• malicious or criminal act • system glitch • human error
Canada, OPC	• accidental disclosure • loss • theft and unauthorised access
NZ, OPC (2016 annual report)	• Website problem • Loss/theft of physical file • Loss/theft of portable storage device • Employee browsing • Electronic information sent to wrong recipient • Physical information sent to wrong recipient • Other
Ontario, OIPC	Issues raised: • disclosure, • security, • collection, • general privacy issue, • use, • access, • inappropriate access, • disposal, • personal information

UK, ICO	• Loss or theft of paperwork, • Data posted or faxed to incorrect recipient • Data sent by email to incorrect recipient • Insecure webpage (including hacking) • Loss /theft of unencrypted device • Insecure disposal of paperwork • Failure to redact data • Information uploaded to webpage • Verbal disclosure • Insecure disposal of hardware • Other failure

Comment by author: Classification of breach types

The classifications fall into three groups:

- High level generic classifications (exemplified by Australia's and Canada's 3 basic types contrasting intentional human acts with system errors).
- Concrete 'down to earth' classifications drawn from the examples before the authority and making further distinctions based upon the media on which data were held (exemplified by the 7-11 types identified by NZ and UK).
- Classification based upon the privacy principles breached in the particular case (as used in Ontario and common in the complaints statistical reporting of many privacy authorities).

The high level classifications might be more likely to endure without change in the long term and be suited to any jurisdiction. However, the more detailed classification may perhaps be more helpful to privacy authorities wishing to identify trends or use the statistics in advocacy and reporting to stakeholders.

Part B: Scope for improvement of breach notification statistics

Stepping beyond current practice, 3 open ended questions were asked:

- What are the primary barriers to collection and sharing of statistic information on breach notification in your view?
- What statistics/measures in relation to breach notification that are not currently available might be most useful to your authority?

The following comments were received:

Respondent authority	Barriers to collection and sharing statistics	New useful measures
Australia, Office of the Australian Information Commissioner	Inconsistency of information reported by notifiers (and incomplete knowledge at time of notification); wide variety of breaches.	-
Canada, Office of the Privacy Commissioner of Canada	As breaches are self-reported by organizations, their officials need to be able to recognize a breach and know where and how to report one. Lack of awareness of requirements is an ongoing concern.	Public sector: risk impact assessment ratings (risk to individual and to institution) to help us better understand how institutions apply the policy's reporting requirements and best target outreach and guidance activities.
Greece, Hellenic Data Protection Authority	It is of ultimate importance to define relevant metrics, so as to have universally comparable statistics. Another factor would be the establishment of a means to disseminate statistics. An additional factor would be the extent to which data controllers will respond to their data breach notification obligation.	In case of serious data breach incidents, if manageable, our DPA would conduct an inspection/audit in order to get all information needed. Supposing, our DPA can't conduct inspections of all data breach incidents, then statistics on the activity sector of the data controller, the data items leaked, the technical problems, the potential impacts and the measures taken would be of utmost importance.
Korea, Korea Internet & Security Agency	Korea has general law on personal data protection, PERSONAL INFORMATION PROTECTION ACT, and also has special law, ACT ON PROMOTION OF INFORMATION AND COMMUNICATIONS NETWORK UTILIZATION AND INFORMATION PROTECTION. According to law, The department of government is different.	None.
Latvia, Data State Inspectorate	Until now we don't get so much breach notifications that we could collect statistical information. According to national law (Electronic Communication Law, available in Latvian: https://likumi.lv/doc.php?id=96611 - the Law in English found at the same webpage section Tulkojums) there is specific cases when electronic communications merchant shall notify Data State Inspectorate regarding circumstances and essence of the breach of personal data protection (Mentioned law, section 68.2).	According to New General Data Protection Regulation which will be applicable from next year, not only electronical communications merchant will be obliged to notify in case of data breach. From Data State Inspectorate side it will give more stronger and useful control in this field.
Mauritius, Data Protection Office	Reluctance to notify breach	Breach Notifications by Category and Type of data controllers
New Zealand, Office of the Privacy Commissioner	Legacy systems	Which party notified (e.g. originator/affected party/third party)
Ontario, Office of the Information and Privacy Commissioner	The main barrier is that breach notification is either not mandatory or, where it is mandatory, undefined. In Ontario notification is voluntary for government institutions but mandatory for health care practitioners; however, even for health care practitioners, it is still voluntary in practice as the threshold for what constitutes a breach has not yet been defined by regulation.	Not applicable. If / when breach notification becomes mandatory, the IPC will define the elements of information that organizations will be required to submit.

Respondents were invited to offer suggestions for reporting and sharing of breach notification statistics. Comments included:

- ‘While breaches are defined similarly in most jurisdictions, there are differing thresholds for reporting which may impact the comparability of the data. Definitions /reporting thresholds may be useful to ensure relative comparability.’
- ‘It may be too early to suggest it, but I think that in the long term a few privacy related statistics might be added to the regular statistics compiled by national statistical authorities, where DPAs may be as data sources or members of the whole statistical system. Until then, the ICDPCC or the European Barometer may serve as means for sharing breach notification statistics.’
- ‘Companies do not like disclosure and personal data breach notification because they can affect their image but if they switch their think that security or protection of personal data is mandatory thing to run a business, and if they think reporting and sharing of breach notification facilitates corporate profit-making finally, usage of statistics on personal data breach notification will increase.’
- ‘Use STIX (Structured Threat Information Expression)’
- ‘It would be very helpful to have a consistent set of measures and definition of organization types (public-sector, private-sector, health) for the collection and reporting of breach notification statistics across jurisdictions.’

Comment by author: Overall

This simple survey has been useful for illustrating a few aspects of ‘real world’ practice of selected privacy and data protection authorities in generating, using and disseminating breach notification statistics. Its usefulness is somewhat limited by some poorly drafted questions and the relatively small number of responses. However, if it were desired to undertake a more detailed study of authority practice the survey results may provide a useful starting point.

A few areas where supplementary research might be useful:
- How closely tied to complaints functions is a role of receiving breach notifications?
- What non-statistical information is kept and released about breach notification?
- Are there concrete examples of the use of the statistics generated?
- Which other regulatory/oversight bodies are involved with breach notification and what are their statistical practices?
- Is the data shared with researchers or other regulators and, if so, what has been revealed?

It appears that there is little commonality in the ways authorities characterise the breaches notified to them (the one exception would seem to be the common practice of dividing the public and private sector breaches). There would appear to be good scope for work to assist authorities to develop common practices for classifying the nature of breaches as well as various other common elements of statistical practice. Such work might both enable the creation of internationally comparable metrics and also help authorities better achieve the several domestic objectives that they have mentioned as the reasons for maintaining such metrics.

Attachment1: Text of Survey

SURVEY ON IMPROVING THE MEASUREMENT OF DIGITAL SECURITY INCIDENTS (PRIVACY AUTHORITY PERSPECTIVES): TAKING STOCK AND PRIORITIES FOR ACTION

Partly in the capacity as convenor of both the ICDPPC Data Protection Metrics Working Group and of the APPA Working Group on Comparative Privacy Statistics, Blair Stewart of the New Zealand Privacy Commissioner's Office has been invited to participate in, and address, an OECD workshop (EXPERT WORKSHOP ON IMPROVING THE MEASUREMENT OF DIGITAL SECURITY INCIDENTS AND RISK MANAGEMENT: TAKING STOCK OF PROGRESS AND PRIORITIES FOR INTERNATIONAL ACTIONS) in May.

While the workshop ranges over various aspects of 'digital security incidents' it is understood that the practical focus will be measurement of breach notification. Earlier (and ongoing) OECD work has concentrated upon cyber-security statistical reporting by CERTs but the current focus, with greater data protection and privacy-relevance, is upon what we might commonly call 'breach notification' or 'data breach notification'.

The OECD workshop particularly brings together experts having either cyber-security or insurance perspectives. To enable Blair to provide more complete information to the workshop from the perspective of privacy and data protection regulators it would be appreciated if members of the ICDPPC and APPA working groups could complete the following survey by 12 April. The survey is tailored to the expected content of the workshop.

Please keep answers brief and provide links if available. For this exercise try to keep focused upon your perspective as a privacy and data protection regulators, i.e. rather than seeking to anticipate the needs of industry, governments, CERTs, insurers, etc.

1. Please name your authority

PART A: Current availability of breach notification statistics in your jurisdiction

2. Is there a voluntary or mandatory breach notification obligation in your jurisdiction under which breaches are notified to your authority?

○ Yes ○ No

If No, please skip questions 2 – 7

3. Do you currently maintain an internal statistical database of the breaches notified to your authority?

○ Yes ○ No

4. If yes,
    a. Why do you keep those statistics and what are they used for?
    b. What measures/statistics do you keep?

5. Do you make any reports outside your authority that draw upon statistics of the breaches notified to your authority?

○ Yes ○ No

6. If yes,
   c. To whom do you report and how often?
   d. What measures/statistics are included in those reports?
   e. Do these reports get made public and if so are they online (please provide URL)?

7. Is there a central repository – whether official or unofficial - of breaches notified in your jurisdiction?

○ Yes ○ No

8. If yes,
   f. please provide details of who maintains the statistics and who keeps it and, if it is public, please include URL:
   g. In your opinion, why is the repository maintained
   h. Does your authority use the statistics maintained in the repository?

PART B: Scope for improvement of breach notification statistics

9. What are the primary barriers to collection and sharing of statistic information on breach notification in your view?

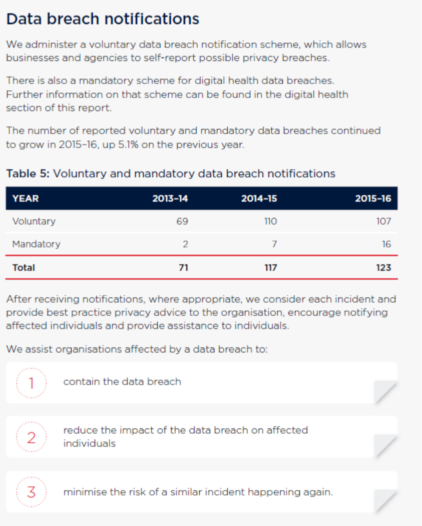
10. What statistics/measures in relation to breach notification that are not currently available might be most useful to your authority?

11. Do you have any suggestions for reporting and sharing of breach notification statistics?

Attachment 2: Illustrative samples of published breach notification statistics etc.

Australia, Office of the Australian Information Commissioner

Annual report



Data breach notifications

We administer a voluntary data breach notification scheme, which allows businesses and agencies to self-report possible privacy breaches.

There is also a mandatory scheme for digital health data breaches. Further information on that scheme can be found in the digital health section of this report.

The number of reported voluntary and mandatory data breaches continued to grow in 2015–16, up 5.1% on the previous year.

Table 5: Voluntary and mandatory data breach notifications

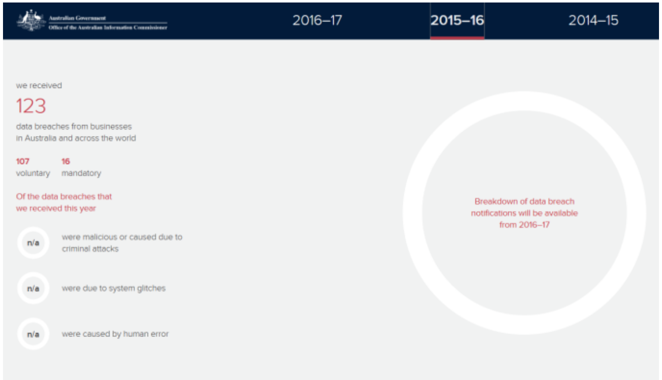
YEAR	2013–14	2014–15	2015–16
Voluntary	69	110	107
Mandatory	2	7	16
Total	**71**	**117**	**123**

After receiving notifications, where appropriate, we consider each incident and provide best practice privacy advice to the organisation, encourage notifying affected individuals and provide assistance to individuals.

We assist organisations affected by a data breach to:

1. contain the data breach
2. reduce the impact of the data breach on affected individuals
3. minimise the risk of a similar incident happening again.

Performance portal



we received

123

data breaches from businesses in Australia and across the world

107 voluntary

16 mandatory

Of the data breaches that we received this year

n/a were malicious or caused due to criminal attacks

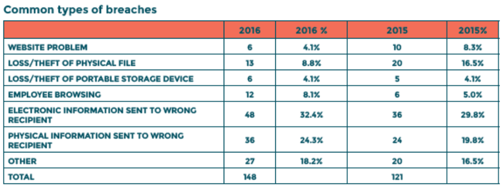
n/a were due to system glitches

n/a were caused by human error

Breakdown of data breach notifications will be available from 2016–17

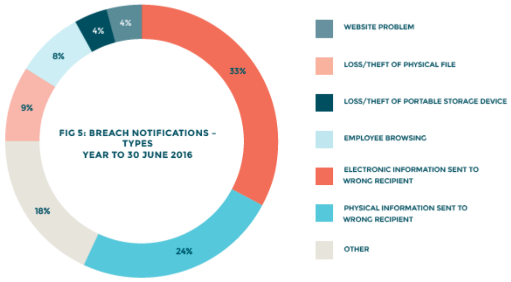
New Zealand, Office of the Privacy Commissioner

Annual report



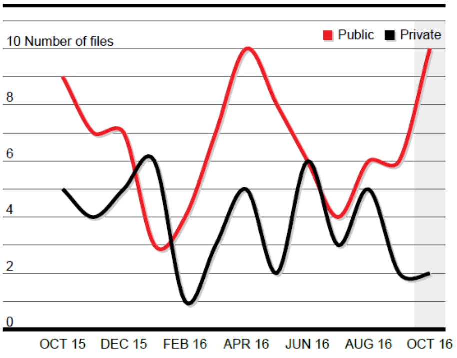
Common types of breaches

	2016	2016 %	2015	2015%
WEBSITE PROBLEM	6	4.1%	10	8.3%
LOSS/THEFT OF PHYSICAL FILE	13	8.8%	20	16.5%
LOSS/THEFT OF PORTABLE STORAGE DEVICE	6	4.1%	5	4.1%
EMPLOYEE BROWSING	12	8.1%	6	5.0%
ELECTRONIC INFORMATION SENT TO WRONG RECIPIENT	48	32.4%	36	29.8%
PHYSICAL INFORMATION SENT TO WRONG RECIPIENT	36	24.3%	24	19.8%
OTHER	27	18.2%	20	16.5%
TOTAL	148		121	



Website snapshot

Breach notifications

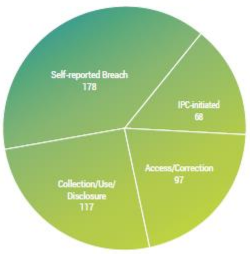


This shows the trend in breach notifications relating to public and private entities.

Ontario, Office of the Information and Privacy Commissioner
Annual report

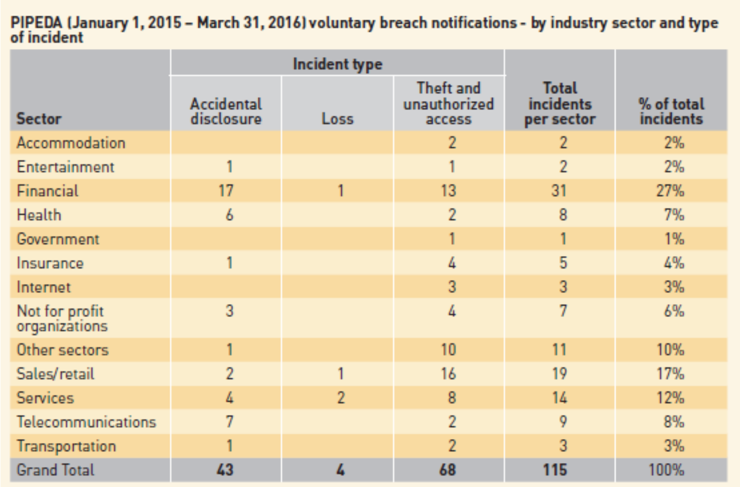
HEALTH PRIVACY

SUMMARY OF PHIPA COMPLAINTS OPENED



Office of the Privacy Commissioner of Canada

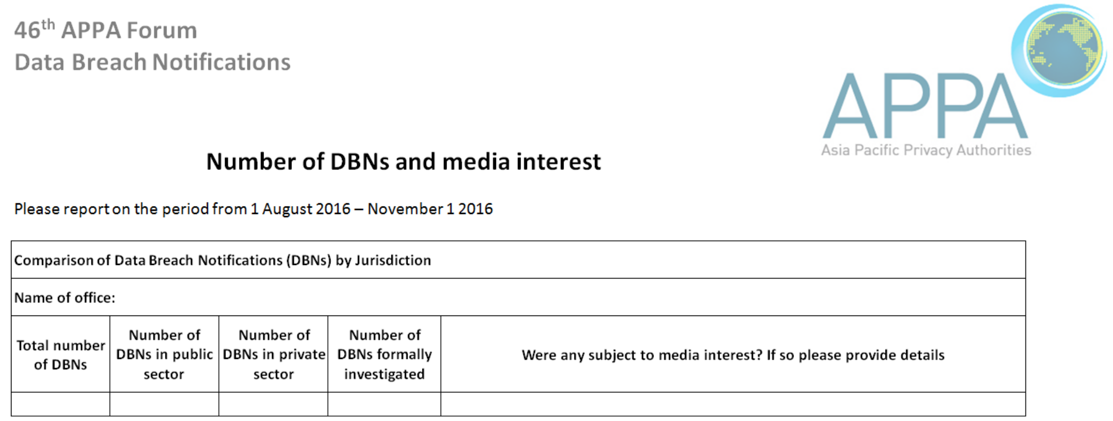
Annual Report
(figures for private sector)



PIPEDA (January 1, 2015 – March 31, 2016) voluntary breach notifications - by industry sector and type of incident

	Incident type				
Sector	Accidental disclosure	Loss	Theft and unauthorized access	Total incidents per sector	% of total incidents
Accommodation			2	2	2%
Entertainment	1		1	2	2%
Financial	17	1	13	31	27%
Health	6		2	8	7%
Government			1	1	1%
Insurance	1		4	5	4%
Internet			3	3	3%
Not for profit organizations	3		4	7	6%
Other sectors	1		10	11	10%
Sales/retail	2	1	16	19	17%
Services	4	2	8	14	12%
Telecommunications	7		2	9	8%
Transportation	1		2	3	3%
Grand Total	**43**	**4**	**68**	**115**	100%

APPA Forum DBN reporting template
(statistical portion used for 46th meeting)



46th APPA Forum
Data Breach Notifications

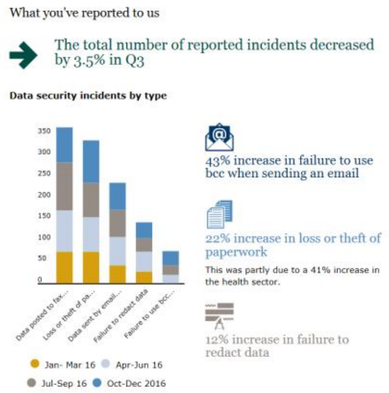
APPA
Asia Pacific Privacy Authorities

Number of DBNs and media interest

Please report on the period from 1 August 2016 – November 1 2016

Comparison of Data Breach Notifications (DBNs) by Jurisdiction				
Name of office:				
Total number of DBNs	Number of DBNs in public sector	Number of DBNs in private sector	Number of DBNs formally investigated	Were any subject to media interest? If so please provide details

ICO, UK
Data security incident trends (website report, extract viewed April 2017)



What you've reported to us

The total number of reported incidents decreased by 3.5% in Q3

Data security incidents by type

43% increase in failure to use bcc when sending an email

22% increase in loss or theft of paperwork

This was partly due to a 41% increase in the health sector.

12% increase in failure to redact data

Attachment 3: Acknowledgments

The author acknowledges the assistance of the following people:

- Office of the Privacy Commissioner, New Zealand
- ICDPPC Data Protection Metrics Working Group
- APPA Comparative Privacy Statistics Working Group
- Staff from the following authorities: Korea Internet & Security Agency; Data State Inspectorate (Latvia); Office of the Privacy Commissioner of Canada; Data Protection Office, Mauritius; Personal Information Protection Commission, Korea; Information Commissioner's Office, UK; Information and Data Protection Authority, Albania; Office of the Information and Privacy Commissioner of Ontario, Canada (IPC); National Privacy Commission, Philippines; Hellenic Data Protection Authority; Office of the Australian Information Commissioner; Office of the Privacy Commissioner, NZ.