OECD EXPERT WORKSHOP ON
IMPROVING THE MEASUREMENT OF
DIGITAL SECURITY INCIDENTS AND RISK MANAGEMENT
TAKING STOCK OF PROGRESS AND PRIORITIES FOR INTERNATIONAL ACTIONS

Zurich, 12-13 May, 2017

Panel II: Challenges and Opportunities of incident disclosure obligations

A Privacy Authority Perspective

Blair Stewart, Assistant Privacy Commissioner, New Zealand

Also presenting as convenor of:
ICDPPC Data Protection Metrics Working Group
APPA Forum Comparative Privacy Statistics Working Group

Back to basics:

Roles of a Data Protection Authority

Data protectors as …		
1 Ombudsmen	2 Auditors	3 Consultants
4 Educators	5 Negotiators	6 Policy advisers
7 Enforcers	Source: C Bennett & C Raab, *The Governance of Privacy: Policy Instruments in a Global Perspective*, 2003	

- DPAs are statutory bodies so need to link activities (like gathering or publishing statistics) to their official functions.
- DPAs' intrinsic 'multi-faceted regulator' nature should lend itself to applying the insights gained from statistics generated in one capacity to other roles.
- DPAs should be a prime producer and consumer of good statistical information on security incidents and risks affecting personal data.

Recent breach notification data from DPA community: ICDPPC Census (1/3)

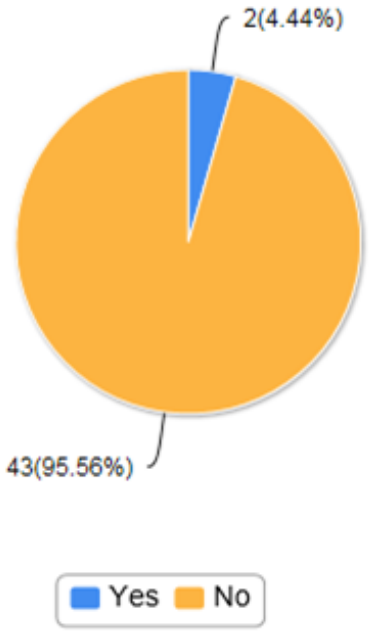
- ICDPPC Census – 1st survey of 115 DPAs currently under way, results should be available in June
- 5 questions (+ supplementary clarification) on breach notification
- Results in from 71 DPAs so far, not analysed

Some interim results from ICDPPC Census (2/3)

- Two thirds of respondents authorities (47/71) have mandatory breach notification laws in their jurisdiction
- 76% of those mandatory breach notification laws require notification to both the data subject and the DPA (19.5% only to the DPA with the remaining 4.5% only to the individual concerned)
- The majority of respondent DPAs (56%) had a role in enforcing data breach regulations

Selected interim breach notification results from ICDPPC Census: cross-border notification (3/3)

Do [your mandatory breach notification] requirements provide any explicit direction on notification to individuals living in other jurisdictions?



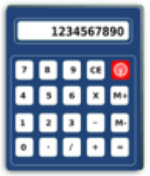
SEM to OECD Privacy Guidelines 2013 suggest that “when designing … breach notification requirements, special consideration … be given to the interests of affected individuals who may live outside the jurisdiction”

Recent breach notification data from DPA community: WG survey (1/6)

- In March/April 2017 a survey undertaken with cooperation of:
  - ICDPPC Data Protection Metrics Working Group
  - APPA Comparative Privacy Statistics Working Group
- To explore how statistics relating to breaches notified to DPAs are kept, used and disseminated
- Full results available at: https://icdppc.org/wp-content/uploads/2017/04/Breach-notification-statistics-survey-report-18-April-2017.pdf

ICDPPC
International Conference of Data Protection & Privacy Commissioners

Data Protection Metrics *Working Group*



APPA
Asia Pacific Privacy Authorities

Selected findings of survey of DPA breach notification statistical practices (2/6)

Results principally based on reported practices of 8 DPAs:

- Separate systems not generally created for breach notification statistics – often grafted onto existing complaints and investigations case management systems
- Several DPAs solicit notifications with online templates which are well suited to standardising statistics
- 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.).

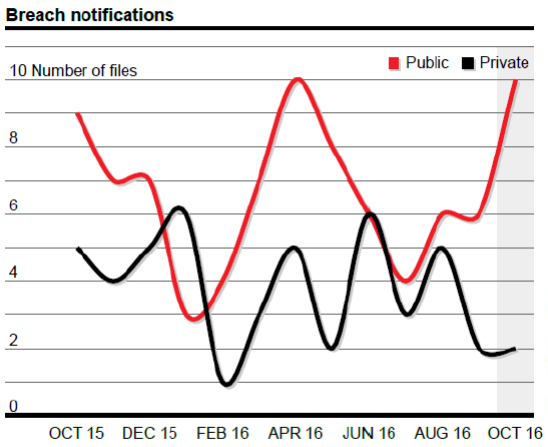
Selected findings of survey of DPA breach notification statistical practices (3/6)

- Statistical reporting evolving e.g. with experience or on transition from voluntary to mandatory reporting
- Suggested uses of the statistics:
  - 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').

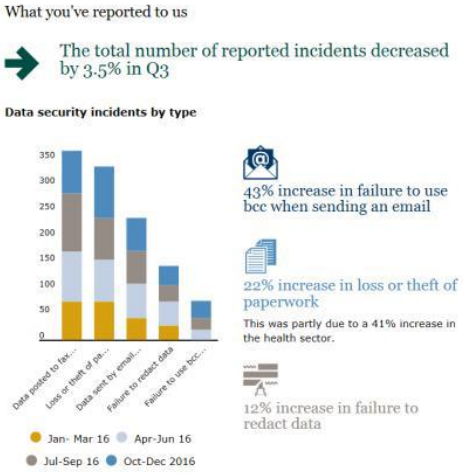
Selected findings of survey of DPA breach notification statistical practices (4/6)

- Privacy authorities periodically provide statistical reports to relevant governance bodies (e.g. responsible government Minister, legislature). Some post 'dashboard' type reports to their website.

Website snapshot



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



Performance portal

Selected findings of survey of DPA breach notification statistical practices (5/6)

DPA Purposes suggested for statistical repositories:

- Archival responsibilities
- To directly support breach management
- To provide a broader or longer term view

Classification of breach type:

- High level generic classifications
- Concrete ‘down to earth’ classifications drawn from the examples
- Classification based upon privacy principles

Selected findings of survey of DPA breach notification statistical practices (6/6)

Areas identified for supplementary research:

- 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?

Challenges/opportunities from a DPA POV in achieving internationally comparable metrics in breach notification

Opportunities

- Majority of DPA jurisdictions now have breach notification laws and DPA has role in receiving notices and enforcing requirements
- Many are in implementation mode – 2017/18 will see many new laws commence
- DPAs as both source and user of comparative statistics – and can apply insights across a range of enforcement, policy advice & public education roles
- ICDPPC could assist in promulgating approaches recommended by OECD

Challenges/opportunities from a DPA POV in achieving internationally comparable metrics in breach notification

Two challenges

- Variances in laws
- Interconnections with statutory functions, esp. complaints handling

Blair Stewart

Assistant Commissioner (Auckland)

Office of the Privacy Commissioner, New Zealand

Blair.Stewart@privacy.org.nz

ICDPPC Secretariat

ExCoSecretariat@icdppc.org