Data Breach Code of Practice

Diarmuid Hallinan
Office of the Data Protection Commissioner
Ireland

ENISA Workshop on Data Breach Notification
24 January, 2011

An Coimisinéir Cosanta Sonraí

Data Protection Commissioner

Presentation Outline

- Why a Code?
- Main Provisions
- Our experience of the Code

An Coimisinéir Cosanta Sonraí

Data Protection Commissioner

Data Security Concerns

- Exponential growth in personal data holdings
- Increased outsourcing
  - *3rd countries*
  - *"cloud" providers*
- Data Breach Scandals
  - *Evidence inadequate controls*

Security bre
raises conce
about safety of

Group set up to inquire into
Social and Family Affairs leaks

vant
lata

o abuse

Probe launched
into civil servant
leak to criminal

to criminal

e

brother

Data chiefs
launch probe

Public's information will be
safe, says data commissioner

Official gave private details

Conroy: officers face action if data accessed without good reason

to media in new leak shock

Department employee resigns after accessing records of 40 people

dog's

leaked d

to

Govt info

vow to stop
your details

Six officials probed over leaks

g leaked

An Coimisinéir Cosanta Sonraí Data Protection Commissioner

DPA Security Provisions (S2 & 2C)

- "Appropriate security measures" to prevent "unauthorised access to, or unauthorised alteration, disclosure or destruction of, the data and against their accidental loss or destruction"
- "Provide a level of security appropriate to.. the harm that might result … and .. the nature of the data concerned"
- "May have regard to the state of technological development and the cost of implementing the measures"

An Coimisinéir Cosanta Sonraí Data Protection Commissioner

Official Response

- Department of Finance Guidelines for Public Service
- M/Justice Working Group
- Data Breach reporting obligation in new EU *e*Privacy Directive

An Coimisinéir Cosanta Sonraí Data Protection Commissioner

Working Group Report

- Gross breaches of DP Principles (including Security) should be an Offence
  - *Minister will consider in the light of EU developments*
- Breach reporting obligations in statutory Code of Practice
  - *Code approved by DPC 7 July 2010, following consultation*
  - *Submitted to Minister for statutory process*

An Coimisinéir Cosanta Sonraí Data Protection Commissioner

Code Documentation

- Personal Data Security Breach Code of Practice
- Breach Notification Guidance
- Data Security Guidance (Updated)
  - *All on www.dataprotection.ie*

An Coimisinéir Cosanta Sonraí Data Protection Commissioner

Why a Code?

- Protect Rights of Individuals
  - *"..focus of the Office of the Data Protection Commissioner in such cases is on the rights of the affected data subjects in relation to the processing of their personal data.." (*Code*)*

- Promote better Data Security
- Provide DPC with relevant Information to advise Organisations

An Coimisinéir Cosanta Sonraí

Data Protection Commissioner

Presentation Outline

- Why a Code?
- **Main Provisions**
- Our experience of the Code

An Coimisinéir Cosanta Sonraí Data Protection Commissioner

What is Covered?

- *"..risk of unauthorised disclosure, loss, destruction or alteration of personal data ..")*(Code*)*
- "..*It is not just lost USB keys/disks/laptops. It may include any loss of control over personal data entrusted to organisations, including inappropriate access to personal data on your systems or the sending of personal data to the wrong individuals..")* (Data Breach Guidance)

An Coimisinéir Cosanta Sonraí

Data Protection Commissioner

Informing Data Subjects

- Key focus of Code:
  - *"..Such information permits data subjects to consider the consequences for each of them individually and to take appropriate measures .."*
  - *" ..In appropriate cases, data controllers should also notify organisations that may be in a position to assist in protecting data subjects including, where relevant, An Garda Síochána (police), financial institutions etc..* (Code)
  - *[May be delayed at police request]*

An Coimisinéir Cosanta Sonraí

Data Protection Commissioner

Information to Data Subjects

- Nature of Breach
- Contact Point
- Advice to mitigate harm
- Channel of Communication depends on circumstances
  - *Individual*
  - *Public*

An Coimisinéir Cosanta Sonraí Data Protection Commissioner

Initial Report by Data Controller to DPC

- Within 2 working days of incident
- by e-mail (preferably), telephone or fax
- Basic facts and measures being taken
  - *Must not include personal data*

An Coimisinéir Cosanta Sonraí Data Protection Commissioner

Detailed Report to DPC (if requested)

- *the amount and nature of the personal data that has been compromised;*
- *the action being taken to secure and / or recover the personal data that has been compromised;*
- *the action being taken to inform those affected by the incident or reasons for the decision not to do so;*
- *the action being taken to limit damage or distress to those affected by the incident;*
- *a chronology of the events leading up to the loss of control of the personal data; and*
- *the measures being taken to prevent repetition of the incident*

An Coimisinéir Cosanta Sonraí Data Protection Commissioner

Reporting Exemptions (1)

- No need to notify **Data Subjects or DPC** "…*If the data concerned is protected by technological measures such as to make it unintelligible to any person who is not authorised to access it* …" (Code)
  - *E.G. Laptop with strong password and encryption* (Breach Notification Guidance)

An Coimisinéir Cosanta Sonraí Data Protection Commissioner

Reporting Exemptions (2)

- **<u>No need to report to DPC</u>** if:
- Reported fully and promptly to Data Subjects **and**
- Does not affect more than 100 Data Subjects **and**
- Does not include ***sensitive*** or ***financial*** data
  - *Financial: last name plus account or card number*
- If in doubt, report

An Coimisinéir Cosanta Sonraí Data Protection Commissioner

Internal Record-Keeping

- Summary Report:
  - *Brief Description of Incident*
  - *Why DPC not notified (if applicable)*
  - *Available for inspection by DPC*

An Coimisinéir Cosanta Sonraí

Data Protection Commissioner

Data Processors

- Must report to Data Controller
- Data Controller to act in accordance with Code

An Coimisinéir Cosanta Sonraí Data Protection Commissioner

Action by DPC

- May carry out fuller investigation
- May recommend that Data Subjects be notified (if not already done)
- Use enforcement powers if necessary

An Coimisinéir Cosanta Sonraí

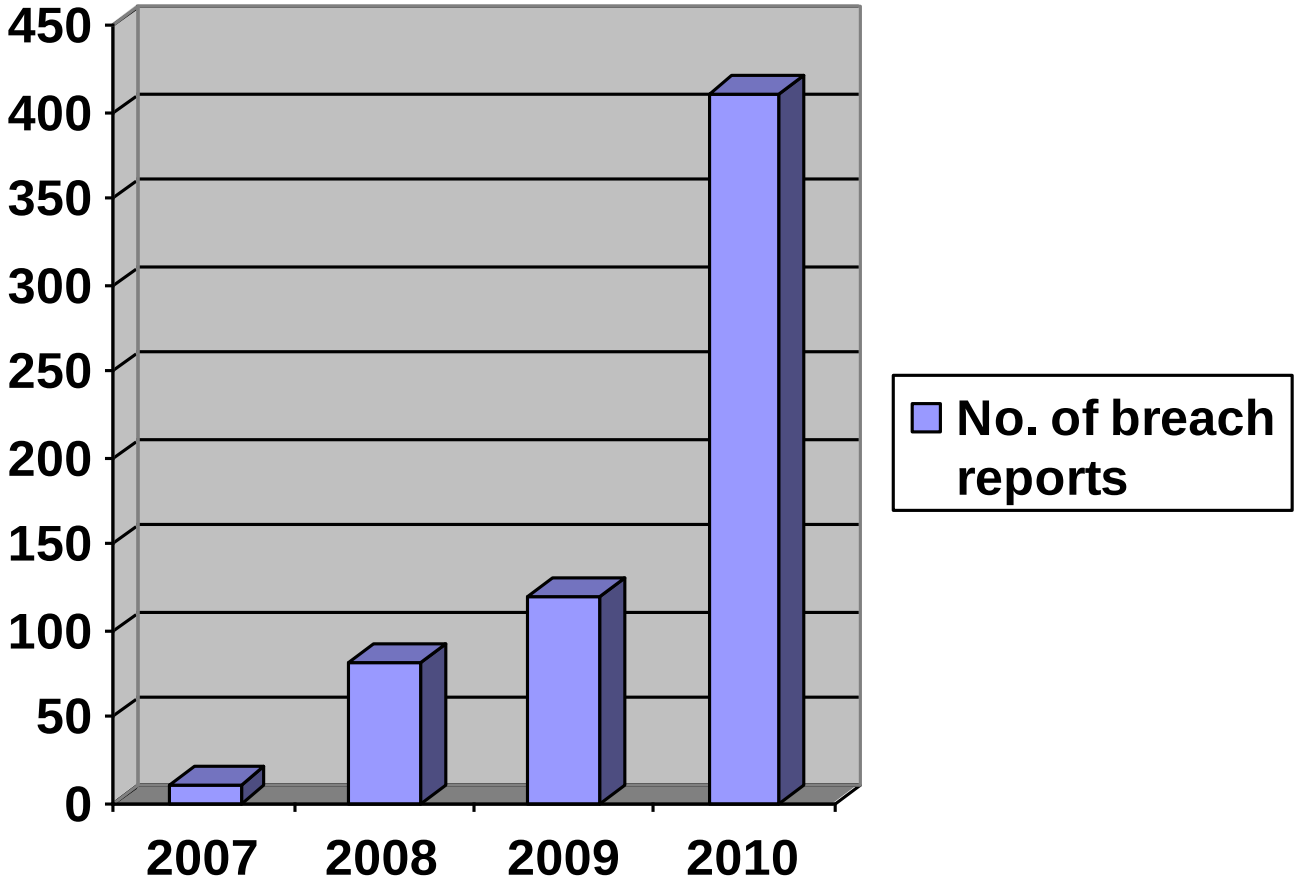
Data Protection Commissioner

Presentation Outline

- Why a Code?
- Main Provisions
- **Our experience of the Code**

An Coimisinéir Cosanta Sonraí Data Protection Commissioner

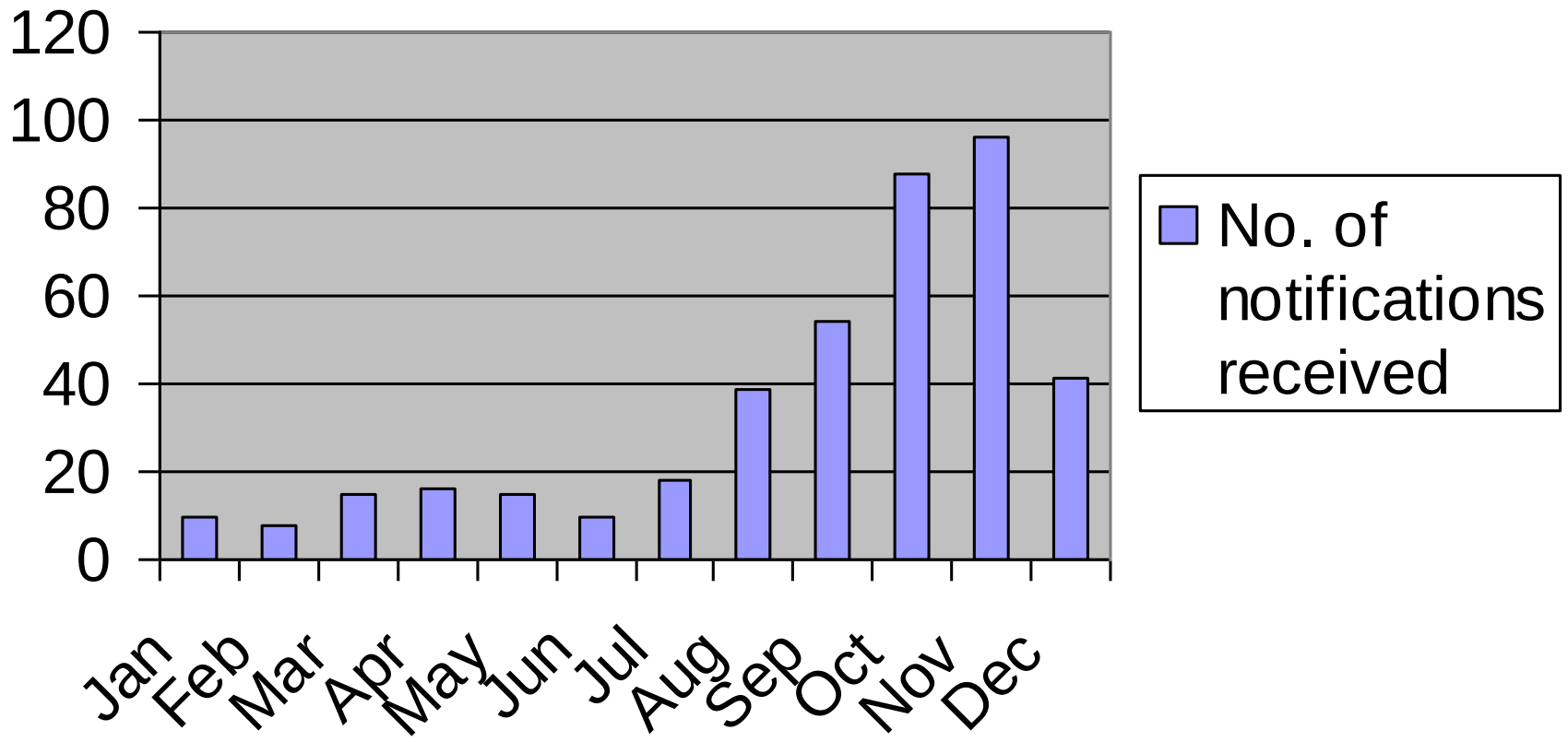
Trends



An Coimisinéir Cosanta Sonraí

Data Protection Commissioner

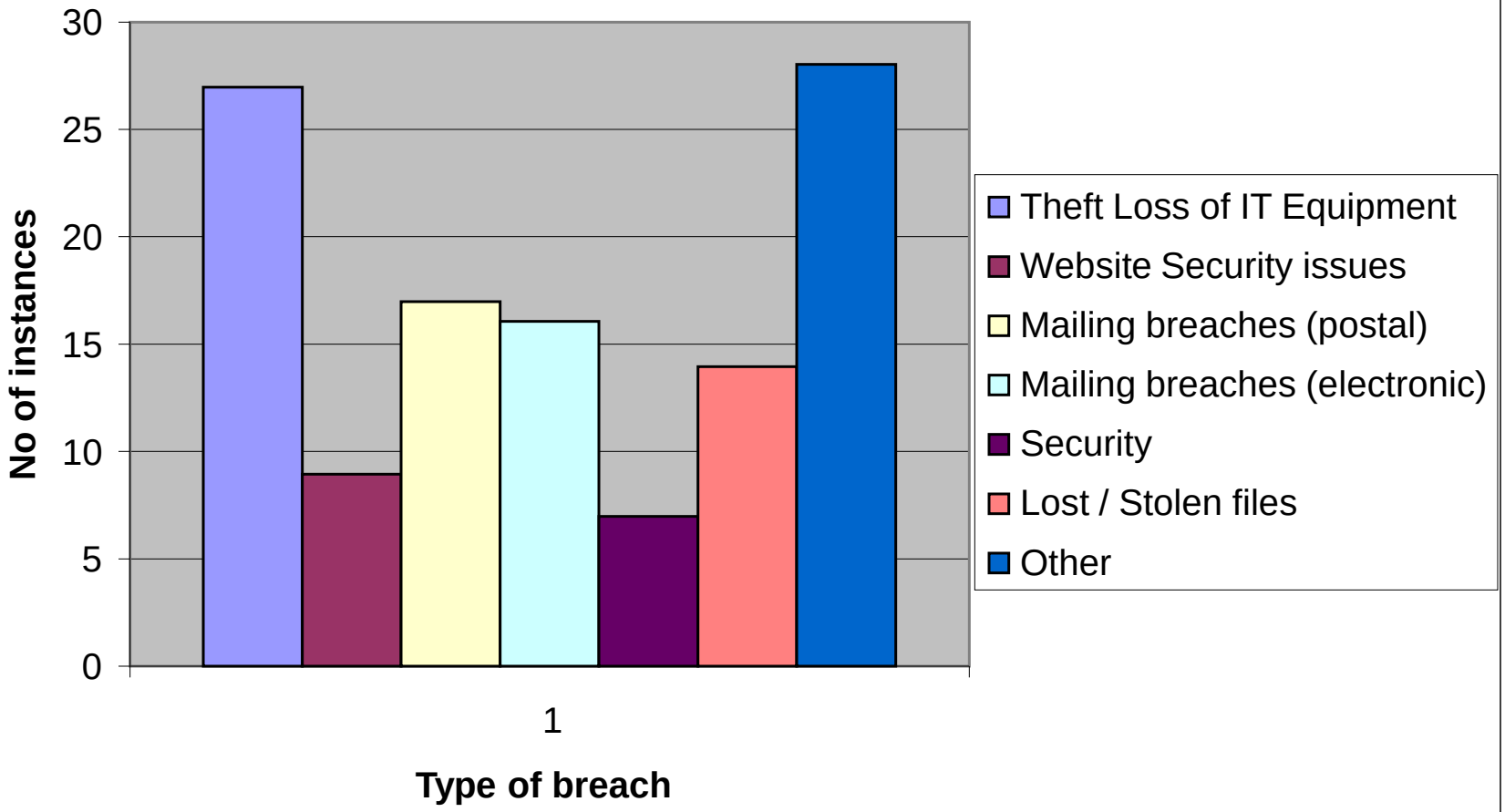
2010 breach notifications received



An Coimisinéir Cosanta Sonraí

Data Protection Commissioner

Data Security Breaches - by type (2009)



An Coimisinéir Cosanta Sonraí Data Protection Commissioner

Impact of the Code

- High level of compliance given the voluntary nature of the Code
- Compliance issues with smaller organisations
- High levels of reporting from the financial sector (inclusion of "personal data of a financial nature" in the Code)
- Notification patterns indicate problems in the health sector

An Coimisinéir Cosanta Sonraí
Data Protection Commissioner

Thank You

Diarmuid Hallinan
Office of the Data Protection Commissioner
Canal House
Station Road
Portarlington
Co Laois
Ireland

Email: info@dataprotection.ie
Website: www.dataprotection.ie