Data Breach Notifications
The way forward

ENISA Workshop on DBN

Brussels, 24th January 2011

ENISA's role

- Centre of expertise in information security issues
- Facilitates contacts between MSs, EU bodies and industry players
- Switchboard of information for good practices
- Work Streams

Goals of the workshop

- Disseminate results of ENISA study
- Compare views on DBN
  - EU institutions
  - National Data Protection Authorities
  - Industry
- Discuss the way forward

DBN study

- Policy context
  - Review of ePrivacy Directive (2002/58/EC)
  - Article 4
- Objectives
  - Survey/stock taking
  - Analysis
    - Views and opinions
    - Understanding of “personal data”
    - Existing other fields models
    - Differences between sectors
    - Undue delay
    - Notification of citizens (if and what)
    - Need of audit mechanisms
    - Benefits from pan-EU approach
  - Conclusions / recommendations
- Methodology

Data Protection Authorities

- Definitions
- Determination of breach
- Determination of risk
- Notification and handling
  - Procedures, triggers, content, delay
- Compliance
  - Enforcement, audits, fines

DPAs – conclusions

- Majority of DPAs support DBN
- Concerns regarding workload
- Need for prioritization
- Need for effective process
- At the time of collecting data, any DPAs in “wait and see” mode

Companies

- General views
- Sources, triggers, content of notifications
- Notifications to Data Subjects
- Relationship with regulators
- Role of DPAs

Companies – conclusions

- Satisfaction of current standards across EU
- Triggers for DBN not clearly defined
- Good awareness of legislation regarding DBN
- High level of confidence in internal procedures
- Concerns about being the only sector obliged for DBN
- Assistance in interpretation of legislation needed

Divergences DPAs / Operators

- Undue delay
  - Regulators: short deadline
  - Operators: identifying and solving the problem as first priority
- Traffic monitoring
  - Regulators: privacy risk
  - Operators: requested to analyze traffic by customers
- Content of notifications
  - Regulators: all necessary information
  - Operators: information not affecting relations with customers
- Audits and role of DPAs
  - Regulators: performing audits is DPAs duty
  - Operators: DPAs should provide guidance and support

Conclusions

- DBN will not contribute in data protection in short term
- DBN will ensure information is given and actions taken
- Problems are not country-specific (cloud!)
- Industry needs clear guidelines
- DPAs need resources

To be discussed

- Technical implementation
  - Notification threshold
  - Risk assessment
  - Procedures
  - Evaluation period
  - Automation
- Other actions?

Thank you! Now let's discuss...

Sławomir Górniak,
European Network and Information Security Agency
Technical Competence Department

Email: Slawomir.Gorniak@enisa.europa.eu

- References
  - http://www.enisa.europa.eu/act/it/dbn
  - http://www.youtube.com/user/enisasta