Data breach notification

4 April 2019

Giuseppe D’Acquisto
Outline

• Statistics
• Workload: past, present, future
• Effectiveness
• A way forward (incentive compatibility, public interest and interplay between art. 32 and art. 33-34)
Statistics

Number of data breach notifications per month

Public entities
Private entities

(*) from 25 May 2018
Statistics

Percentage of data breach notifications by data controller type

- Private entities: 26%
- Public entities: 74%
Percentage of data breach notifications by data controller sector (TOP 10)

- Health: 14.0%
- Education: 13.0%
- Finance, Insurance & Credit: 11.0%
- Online Technology and Telecoms: 10.9%
- Local Government: 8.7%
- Land or Property Services: 4.7%
- Transport and Leisure: 4.4%
- Retail: 4.2%
- Central Government: 3.8%
- Charities: 1.7%

Legend: Private sector • Public sector
Percentage of data breach notifications by incident type

- Hacking: 17.5%
- Mail lost or opened: 13.0%
- Device lost or stolen: 12.2%
- Unintentional publication of information: 8.1%
- Paper lost or stolen: 6.1%
- Malware (e.g. ransomware): 5.1%
- Data sent to wrong recipient: 3.2%
- Ransomware: 1.7%
- Phishing: 0.9%
- Unavailability of processing systems: 0.9%
- Data of wrong data subject shown: 0.5%
- Incorrect disposal of data: 0.1%
- Other: 30.9%
Percentage of data breach notifications in health sector by incident type

- Paper lost or stolen: 18.3%
- Device lost or stolen: 17.2%
- Unintentional publication of information: 12.9%
- Mail lost or opened: 10.8%
- Data sent to wrong recipient: 10.8%
- Malware (e.g. ransomware): 9.7%
- Hacking: 8.6%
- Unavailability of processing systems: 4.3%
- Incorrect disposal of data: 1.1%
- Phishing: 1.1%
- Other: 5.4%
Percentage of data breach notifications in government sector by incident type

- Hacking: 18.3%
- Device lost or stolen: 14.0%
- Mail lost or opened: 9.7%
- Unintentional publication of information: 8.6%
- Data sent to wrong recipient: 4.3%
- Malware (e.g. ransomware): 3.2%
- Paper lost or stolen: 2.2%
- Ransomware: 2.2%
- Unavailability of processing systems: 1.1%
- Other: 10.8%
Percentage of data breach notifications by number of data subjects

- 0 - 49: 46.4%
- 50 - 99: 5.8%
- 100 - 199: 5.8%
- 200 - 499: 19.8%
- 500 - 999: 5.8%
- 1,000 - 1,999: 5.8%
- 2,000 - 4,999: 1.4%
- 5,000 - 9,999: 3.4%
- 10,000 - 49,999: 3.9%
- 50,000+: 1.9%
Percentage of data breach cases by status

- Closed: 31.1%
- Open (assigned to IT Dept.): 61.0%
- Open (assigned to Legal Depts.): 7.9%
Statistics

Age of data breach cases open as of 28 February 2019

- 0 - 30 days: 16.6%
- 31 - 90 days: 24.3%
- 91 - 180 days: 37.6%
- 181+ days: 21.5%
Relative percentage of data breach cases closed within three timeframes

- 30 days or less: 20.3%
- 90 days or less: 73.4%
- 180 days or less: 91.4%
Statistics: some Italian DPA numbers

Percentage of data breach cases by investigation steps

0 step 59.4%
1 step 31.2%
2 steps 6.3%
3 steps 1.8%
4 steps 0.6%
5+ steps 0.6%
Workload: past, present, future

• 56% of businesses have suffered at least one security incident within the last year (Ponemon Institute, 2018)

• Let’s make some computations
  – According to the national statistic bureau (ISTAT) in Italy we have 4 Million businesses
  – We should expect 2 Million security incidents
  – How many notified in 1 year? 2000 (conservative estimate)
Workload: past, present, future
Workload: past, present, future

- Unknown events
- Negligence (art. 32)
Workload: past, present, future

- Workload data breach
- Workload other activities

- Pre-GDPR (e-privacy)
- Peak of the iceberg
- Full iceberg
Effectiveness

- Negligence
- Investigate
- Discard
Effectiveness

• When we discard
  – We assess the risk (where is accountability?)
  – We give «on call» assistance (not exactly our job!)
  – We open and close a formal case

• When we investigate
  – We can prescribe technical and organizational measures (requiring investments)
  – We can prescribe the communication of the data breach to the affected data subjects (that may impact reputation)
  – We can impose fines (requiring expenditures)
Effectiveness

• Consequences of discarding
  – Workload with poor societal benefit
  – It’s a sort of public audit to private companies
  – Not manageable in «full iceberg» scenario

• When we investigate
  – We observe a slow down in notifications (it’s just a correlation!)
  – DPOs who suggested their controllers to notify are disappointed
A way forward

PLANE CRASH DEATHS
Annual deaths per 10 billion passenger miles, by commercial airlines. Five-year averages.

Implementation of a mechanism of disclosure of flight incidents

Source: Gapminder[16] based on IATA, ICAO[3], BTS[1,2] & ATAA
A way forward

Notification in the public interest (of gaining knowledge on unknown incidents and increase trust in digital services)
A way forward

Interface  Negligence

Investigation
Conclusions

- Notification is very useful to enhance trust and to protect individual’s rights in data economy
- It is less suited for discovering negligence (few incentives)
- We don’t need to restructure the mechanism, but we need to work on the «notification interfaces»
  - For notification we need trust between DPAs and controllers and very skilled authoritative DPOs
  - For discovering negligence we need to promote users’ role and certification mechanisms, finding the right incentives for disclosure
Thanks

g.dacquisto@gpdp.it