Data Breaches in Greece: Case Studies from HDPA Experience

Hellenic Data Protection Authority

Anargyros Chryssanthou
ICT Auditor
achrysanthou at dpa.gr

Structure of presentation

- Definitions
- Legal Regime
  - Europe
  - Greece
- HDPA Experience
  - Statistics
  - Policy
  - Cases
  - Common Characteristics
- The future

Definitions

Information Security Incident

- "*An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security*" (ISO/IEC 27035:2011)

Data Breach

- "*An unauthorized dissemination of information. It may be due to an attack on the network or outright theft of paper documents, portable disks, USB drives or laptops. Sensitive information can also be found in trash cans when reports are carelessly discarded.*"

(http://www.pcmag.com/encyclopedia_term/0,1237,t=data+breach&i=61571,00.asp)

Personal Data Breach

- *"a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a publicly available electronic communications service in the Community"*

(Directive 2002/58/EC as amended by Directives 2006/24/EC and 2009/136/EC, article 2 edifice h)

Personal Data

- *"any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity"*

(Directive 95/46/EC, article 2 edifice a)

Legal Regime

Europe (1/2)

- First Definition of the term “Personal Data Breach” in Directive 2009/136/EC, amending Directive 2002/58/EC
- Obligation of publicly available electronic communications services providers
  - Notify competent authority without undue delay
  - Notify the subscriber or individual of the breach without undue delay (under specific conditions)
  - Maintain an inventory of personal data breaches

  (Directive 2002/58/EC as amended by Directive 2009/136/EC, article 3)

☞ 25/1/2012 - European Commission proposes a comprehensive reform of the data protection rules

Europe (2/2)

- Data controllers' obligation to notify personal data breaches
  - Supervisory authority (DPA)
  - Data subject
  - Without undue delay
  - In detail
- Data subject right to lodge a complaint
- Universal format and notification procedures
- Possible fine up to 1.000.000 Euros (or up to 2% of annual worldwide turnover) for
  - Notification omission
  - Incomplete / Untimely notification

(European Commission, 2012/0010(COD), articles 3(9), 28-29, 32(e) and 50, 2012/0011(COD), articles 4(9), 30,31, 37 (1e), 73 and 79(6h))

Greece

- Amendments of Directive 2002/58/EC transposed to Greek law with Law 4070/2012 amending Law 3471/2006
- Provisions of notification obligation for telecommunication providers
  - security incidents in general
  - personal data breaches
- Telecommunications providers have to keep a "book" of security incidents and personal data breaches

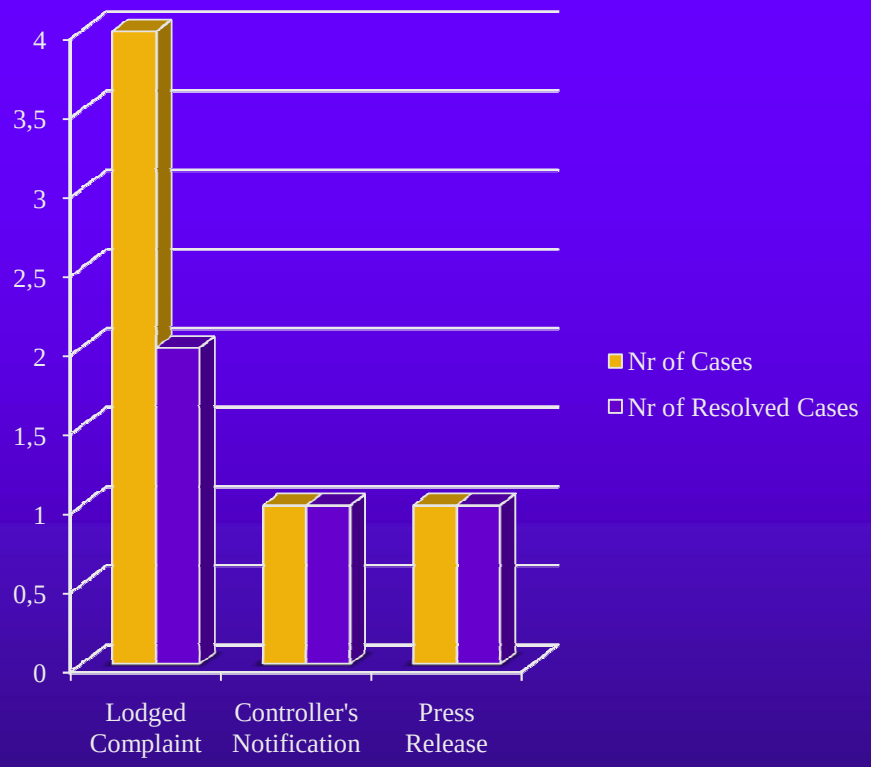
(*Hellenic Authority for Communication Secrecy, Regulation on Ensuring Electronic Communications Secrecy, article 9, Law 4070/2012, article 37 & Law 3471/2006 as amended by Law 4070/2012, article 2 edifice 11, articles 12 edifices 5-10*)

- HDPA handles reported data breaches in the basis of
  - Law 2472/1997, article 10 paragraph 3 -> data controllers
  - Law 3471/2006 as amended by Law 4070/2012, article 2 edifice 11, article 12 edifices 5-10 -> telecommunication providers

HDPA Experience

Statistics

- In the last 3 years
  - 2 warnings imposing adoption of technical measures (Decisions 60/2011 and 87/2011)
  - 1 monetary fine in the amount of 10.000 Euros (Decision 59/2012)
  - administrative audits (3)
  - letters of clarifications (3)



Policy

- HDPA has an unofficial internal policy based on
  - other DPAs policies
  - ongoing discussion on data protection rules reform
- Policy consisting of
  - Set of criteria to examine data breach cases
    - intelligibility of leaked data
    - actual facts (ex. number of data subjects concerned, categories of leaked data, etc.)
    - incident response (ex. documented procedures, mitigation measures taken, notification of data subjects , notification of HDPA, etc)
    - existing information security measures
    - future actions
  - Notification Form prepared, not yet published or used
  - Levels of Severity (High, Medium, Low, Insignificant)

Cases

1. Children's Healthcare Institute (1/2)

- 3 separate files with medical and social welfare data (sensitive data according to Law 2472/1997 art. 2b)
- stored in 4 computers
- protected by personal passwords and an alarm system
- data periodically backed up

DATA WERE SECURE. ALARM WAS ARMED AND READY

- SOMEBODY BROKE IN
- ALARM DID NOT WORK
- COMPUTERS WERE STOLEN
- theft discovered after 2 days
- police notified immediately
- HDPA notified 17 days later

http://www.legaljuice.com/2009/05/life_for_stealing_a_tv_and_a_l.html

1. Children's Healthcare Institute (2/2)

- HDPA asked for clarifications
- Necessary to establish
  - the circumstances of the breach
  - existing security measures
  - mitigation measures
- 2050 data subjects affected
- Inadequate password management
- Data not encrypted
- Sensitive data available to the thief
- Data was recovered
- Data subjects were notified
- HDPA issued a warning
- Institute ordered to take appropriate measures to

http://www.talktalk.co.uk/money/consumer-corner/

2. Insurance fund (1/2)

- Web application
- Accessible by fund's employees and insured workers
- Data breach identified by insured worker
  - receipt of e-mails containing other users' data
- Complaint lodged
- Administrative audit performed

http://www.experian.com/blogs/data-breach/2012/04/03/the-rx-for-medical-breaches

2. Insurance fund (2/2)

- 12 users received other users' data
- Extent of leaked data undetermined
- Insurance fund
  - informed on the breach by complaint
  - not immediate reaction
  - not efficient reaction
- Breach due to technical fault
  - users' notification function left open by data processor
- HDPA issued warning
- Insurance fund ordered to take security measures

http://www.experian.com/blogs/data-breach/2012/04/03/the-rx-for-medical-breaches

3. Communication service provider (1/3)

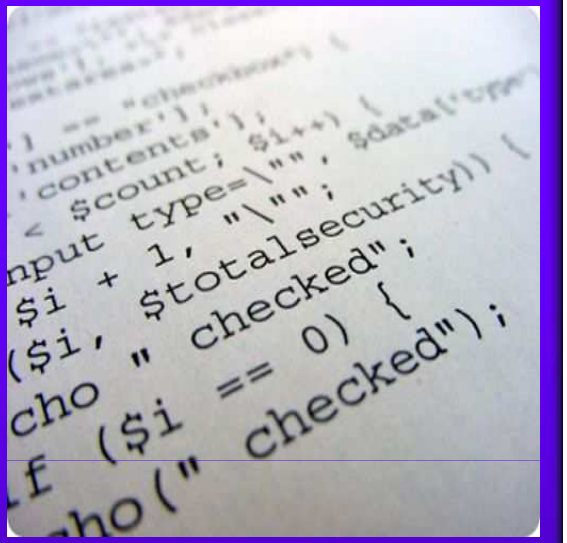
- Phone Number account management web application
- Protected by username and password
- Legitimate user's request to add card-phone numbers to his account
- Access gained to
  - 171 unknown phone numbers
  - numbers dialed
  - account balance
- Complaint lodged to HDPA and to the provider
- Written answer to complainant in 16 days
- Problem corrected
- Administrative audit performed

3. Communication service provider (2/3)

- 12 other users gained similar access, 4 complained
- Complaints
  - not associated
  - not handled as security incidents (no malicious activity present)
- On 5th lodged complaint
  - security manager informed
  - account management application deactivated
  - problem researched and corrected
- Data subjects not informed
- Provider deemed leaked data not personal data
- No logs proving provider's claims

3. Communication service provider (3/3)

- Breach due to technical fault
  - system upgrade
  - previously: 1 customer code –> 1 phone number
  - at time of the breach: 1 customer code –> many phone numbers
  - account management application search function not adjusted
- HDPA
  - deemed leaked data => personal data (Law 2472/1997 article 2 edifice a, Law 3471/2006, article 2 edifice 3)
  - issued recommendations
- Provider ordered to take security measures



http://techgyo.com/index.php/common-types-of-coding-errors/

4. Music Entertainment Company (1/5)

- Web site defaced
- Users' database
  - stolen
  - published on the web
- HDPA informed from web site postings
- Alleged facts
  - method used: hacking through sql injection
  - breach occurred 18 days earlier
- HDPA asked company for clarifications

http://www.allspammedup.com/2012/02/ticketweb-users-hit-with-spam-after-data-breach/

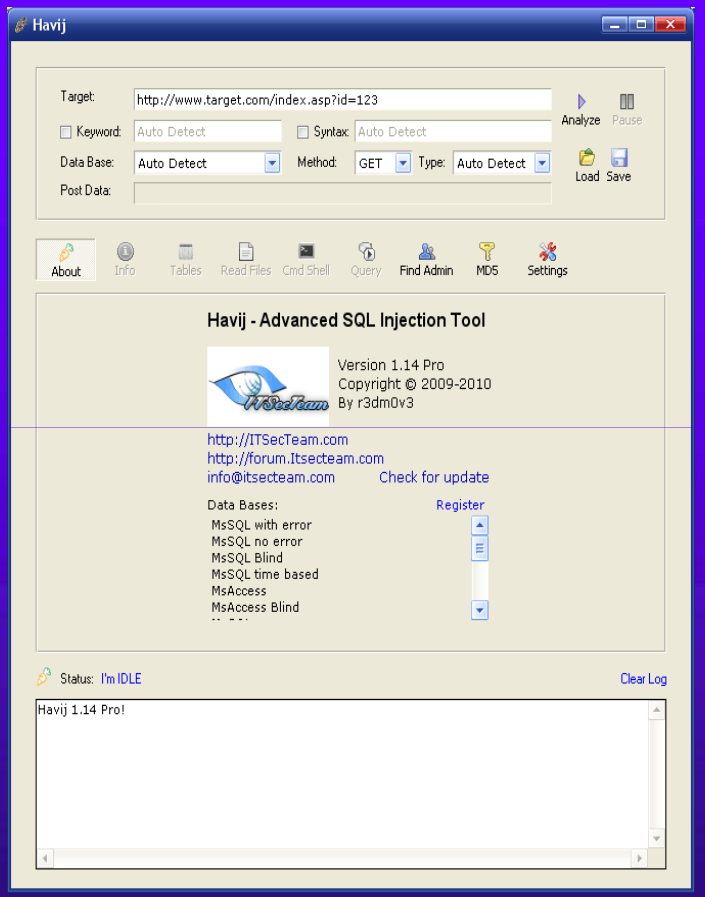
4. Music Entertainment Company (2/5)

- Company replied
  - Date of the breach still under investigation
  - 8385 data subjects affected
  - Leak of simple data including usernames and passwords
  - Website deactivated 17 days after the alleged date of the breach
  - Data subjects informed through multiple web postings
  - Forensic Expert hired
- Administrative audit performed
- Breach circumstances examined
- Digital evidence collected and analyzed

http://www.allspammedup.com/2012/02/ticketweb-users-hit-with-spam-after-data-breach/

4. Music Entertainment Company (3/5)

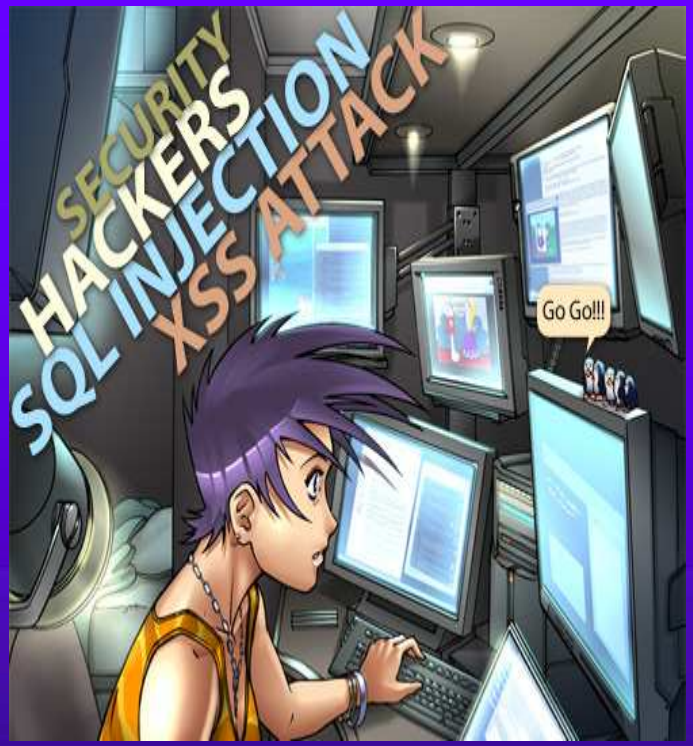
- Findings
  - 3 security incidents
  - 2 defacements
  - 1 defacement 3 years earlier
    - Undetected obfuscated code loading malicious code hosted in website
  - 1 data breach
  - Breach due to hacking through sql injection
  - Hackers used Havij



http://itsecteam.com/en/projects/project1.htm

4. Music Entertainment company (4/5)

- 8385 data subjects affected
- Successful attempts to exploit leaked data
- Website vulnerable to sql injection and cross-site scripting
- Logs kept but not monitored
- Passwords kept unencrypted
- Secure development methods not used
- Site under heavy attack for 3 ½ months



http://www.techmynd.com/kaspersky-bit-defender-facebook-hacked-databases-exposed-sql-injections/

4. Music Entertainment Company (5/5)

- Forensic expert's analysis confirmed breach findings
- HDPA
  - heard company's representatives
  - examined findings
  - took into account security measures were present but not implemented / supported properly
  - leveraged incident response (ex. hiring a forensic expert, taking down postings with breached data, etc) and company's conduct (cooperation with HDPA)
  - deemed company in violation of Law 2472/1997 ar. 10 par. 3
  - imposed 10.000 Euros fine

Common Characteristics

- Majority of Data controllers
  - inadequate security measures in place
  - lack of security – related policies
  - not correctly implemented security measures
  - security – unaware personnel
  - websites / applications unsecure by design
  - websites / applications prone to attacks
  - ineffective incident response
- Jurisdiction issues upon involvement of foreign actors
- Sometimes HDPA faces lack of cooperation

The future

- Data controllers need to be ready
  - legal notification obligation
- Incident response procedures must be
  - documented
  - describing detailed actions to be taken
  - assigning responsibilities
  - setting an incident log format
  - tested with potential incident scenarios
- HDPA ready to assist data controllers
  - in data protection issues by providing guidelines
  - in personal data breaches by giving directions
- Recently HDPA's website was heavily updated (ex. Guidelines document on information security issues)

Useful Links (1/2)

- European Commission's proposals for reforming data protection rules, http://ec.europa.eu/justice/newsroom/data-protection/news/120125_en.htm
- Directive 2009/136/EC amending Directive 2002/58/EC, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:En:PDF
- Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:en:HTML
- Hellenic Data Protection Authority, http://www.dpa.gr
- Law 2472/1997 on Protection of Individuals with regard to the Processing of Personal Data,

  http://www.dpa.gr/portal/page?_pageid=33,123437&_dad=portal&_schema=PORTAL
- Law 3471/2006 on Protection of personal data and privacy in the electronic telecommunications sector and amendment of law 2472/1997, http://www.dpa.gr/pls/portal/docs/PAGE/APDPX/ENGLISH_INDEX/LEGAL%20FRAMEWORK/LAW%203471_06_NOV2011_.PDF

Useful Links (2/2)

- Law 4070/2012, http://www.sedek.gr/gr/attachments/article/133/nom-4070_2012.pdf
- Decision 60/2011 regarding data breach in children's healthcare institute, http://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=123,175,124,84,233,74,18,213
- Decision 87/2011 regarding data breach in an actuarial fund, http://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=100,209,122,228,68,206,76,253
- Decision 59/2012 regarding data breach in a music entertainment company, http://www.dpa.gr/APDPXPortlets/htdocs/documentDisplay.jsp?docid=6,134,204,221,255,182,39,149
- Guidelines document on information security issues, http://www.dpa.gr/pls/portal/url/ITEM/B6F5DCC88FD8EC4AE040A8C07C24572A

Master Slide picture taken from:

- *http://www.bdcon.net/services/data-breach-planning-response.html*

Thank you for your attention