19th HydraMeeting
20-22 September 2017

Matthew Norris,
Underwriter,
Beazley Insurance at Lloyds of London
(UNITED KINGDOM)

HELLENIC ASSOCIATION OF INSURANCE COMPANIES

Thursday, 21.9.2017

Cyber

beazley

Cyber @ Lloyds

https://www.lloyds.om/lloyds/about-us/what-do-we-insure/what-lloyds-insures/cyber

How Cyber Started

- Internet 1998
- Questions about a-virus software and claims from IP
- Notification laws 2003, PCI DSS
- Second wave 2007, TJX
- Property cyber extensions
- PI cyber extensions
- Timescales
- Lessons from the US market
- Regulation

Policy Coverages

Liability

- Privacy
- Infosecurity
- Website content
  - regulatory
  - PCI

requested extensions

1st party
- cyber extortion
- data protection loss
- cyber business interruption

fraudulent transfer

telecom hacking

Service Payment

- Computer Expert Services, legal services & public relations and crisis management
- Notification Services, Call Centre Services and Breach Resolution and Mitigation Services

Types of Data Security Breaches

- **Network Intrusions/Hacks**
- **Malware Viruses**
- **Ransomware**
- **Phishing Attacks**
- **Lost/Missing/Stolen laptops/USBs**
- **Rogue Employees**
- **Duped Employees**
- **Improper Disposal of Data (unintended disclosure)**
  - **Electronic assets**
    - **computers, smart phones, backup tapes, hard drives, servers, copiers, fax machines, scanners, printers**
  - **Paper**
    - **Un-shredded Documents**

Technical vrs human error

Technical Prevention often focus

What is a Data Breach?

- **any** information relating to an identified or identifiable natural person
- "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data"
- Notice is **not required** if "the personal data breach is **unlikely to result in a risk** for the rights and freedoms of natural persons,"
- Notice must be provided "without undue delay and, where feasible, **not later than 72 hours** after having become aware of it."
- Notice must "at least":

  (1) describe the nature of the …breach, including the number and categories of data subjects and personal data records affected;

  (2) provide the data protection officer's contact information;

  (3) "describe the likely consequences of the personal data breach"; and

  (4) describe how the controller proposes to address the breach, including any mitigation efforts.
- Exception if "the data unintelligible to any person who is not authorized to access it, such as **encryption**";

Wide definition | Be quick | Encryption

What Do All Regulators Dislike?

Lack of commitment

Absence of appropriate written policies

Insufficient employee training/awareness

Insufficient dedicated security roles

Failure to address issues identified by risk assessment

Technical

Unencrypted backup tapes

Unencrypted portable devices

Default configurations/passwords

Management

Slow incident detection and notification

Refusal to provide incident reports and forensic investigation report

Details as known
Quorum agreed
Quorum meets
Lawyer
Forensics?

Forensics
What happened
Access to personal data
Is that the only place
Did they export data
What kind of data
When to stop looking
Who is affected
How to stop
How to remediate

Communication
How quickly +/-
Where
What media
What level of detail

Suffering a Data Breach is not a disaster… Mishandling it is.

Offer fraud reporting
For how long
To whom
If fraud ….

Notify?
Contract obligations
Individuals and others
Speak to regulator
Get contact details
Draft email
Set up scripts
Set up call centre

beazley

Data Breaches in Greece

- Insurance fund
  - Technical fault on web application
  - Users received other users' data
  - Audit performed

Not malicious

Routine activity

Security not the focus ?

Data Breaches in Greece

- Music entertainment company
  - Passwords unencrypted
  - Website defaced
  - Sql injection
  - User database stolen and published on web
  - Over 8000 data subjects affected
  - Website deactivated 17 days
  - Logs kept but not reviewed
  - Attacked for 3.5 years
  - Audit peformed
  - 10k fine

Technical = large forensic bill

Slow response

Logs not reviewed

= a fine

Data Breaches in Greece

- **Greek Man Accused of Stealing Data of 9 Million Citizens**
  - The 35-year-old accused was found in possession of the data files that included identity card details, tax numbers, vehicle license plate numbers and home addresses.

Credit monitoring services as government issued ID