Seminar 5 preparation

**Data Breach Case Study**

INTERNET NEWS

APRIL 27, 2011 4:54 AMUPDATED 11 YEARS AGO

Sony PlayStation suffers massive data breach

By Liana B. Baker, Jim Finkle

Read Swinhoe, D., 2020. The 15 Biggest Data Breaches Of The 21St Century. [online] CSO Online.

* What types of data were affected?
  + Customer names, addresses and possibly credit card data belonging to 77 million user accounts in what is one of the largest-ever Internet security break-ins.
* What happened?
  + Sony PlayStation suffers massive data breach. Suspected the hackers entered the network by taking over the PC of a system administrator, who had rights to access sensitive information about Sony’s customers.
* Who was responsible?
  + The Information Commissioner’s Office (ICO) issued the penalty after it found the attack on the Sony PlayStation Network in April 2011 could have been prevented.
* Were any escalation(s) stopped - how?
  + Sony said it has hired an “outside recognized security firm” to investigate.
* Was the Business Continuity Plan instigated?
  + Sony said it learned of the breach in its popular PlayStation Network on April 19, prompting it to shut down the network immediately. The restoration of PlayStation Network and Qriocity online movie and music services would take place on a country by country basis and that it expected the process to be complete by May 31. (france24, 2011)
  + https://www.france24.com/en/20110516-sony-electronics-entertainment-restore-playstation-services-hacking-security-breach
* Was the ICO notified?
  + Yes, The Information Commissioner’s Office, the official watchdog for privacy and data security in the UK, has fined Sony Europe $390,000 under the 1998 Data Protection Act. The investigators determined that Sony's IT security of its customers' privacy was inadequate in a data breach involving the personal details of 77 million customers which, the ICO said, could have been prevented with better user password controls.
* Were affected individuals notified?
  + Sony has notified customers of the breach, it had still not provided information on how user data might have been compromised.
* What were the social, legal and ethical implications of the decisions made?
  + Sony Corp could face legal action across the globe after it delayed disclosing a security breach of its popular PlayStation Network, infuriating gamers and sending the firm’s shares down nearly 5 percent in Tokyo. (Reuters, 2011)

If you had been the ISM for the organisation you selected what mitigations would you have put in place to stop any reoccurrences?

As Paller said Sony probably did not pay enough attention to security when it was developing the software that runs its network. In the rush to get out innovative new products, security can sometimes take a back seat.

ISM for the organisation should review on the developing and preform a security audit. For the sensitive data, should be encrypted before storing in database.