UNIT 4: BREACH ANALYSIS CASE STUDY

CASE 14: ADOBE

DETAILS ABOUT THE BREACH

- **Breach Date:** Early October 2013.
- **Type of Data Affected:** Theft of almost 3 million encrypted customer credit card records

  Login data for an undetermined number of user accounts

  IDs (usernames) and encrypted (hashed) passwords for 38 million users
- **What Happened:** A Data Breach at Adobe where hackers stole and exposed at least 38 million users' sensitive information.

Part of the Adobe breach involved the theft of source code for Adobe Acrobat and Reader, as well as its ColdFusion Web application platform.

Among the cache, was a 2.56 GB-sized file called ph1.tar.gz, but KrebsOnSecurity and Hold Security were unable to crack the password on the archive.

Later on, AnonNews.org posted a non-password protected file by the same name and size that appeared to be source code for Adobe Photoshop.

In late September, Adobe spokesperson, Heather Edell, confirmed that intruders got some of the Photoshop source code and they contacted the sites hosting the data linked to from the AnonNews postings and had the information taken down.

DETAILS ABOUT THE BREACH CONTINUATION 1

- **Were Any Escalation(s) Stopped - How?** Adobe spokesperson Heather Edell confirmed to:
  - Completion of email notification of the affected users.
  - Resetting of the passwords for all Adobe IDs with valid, encrypted passwords that were believed to be involved in the attack.
  - Ongoing notification to inactive Adobe users.
  - Having the information (source code) taken down by contacting the sites hosting the data linked to and from the AnonNews postings
  - Offering a year's worth of credit monitoring to customers whose encrypted credit card data was stolen in the breach.

DETAILS ABOUT THE BREACH CONTINUATION 2

- **Was The Business Continuity Plan Instigated?** Adobe offered a year's worth of credit monitoring to customers whose credit card data was stolen in the breach.
- **Were Affected Individuals Notified:** Adobe spokesperson Heather Edell said that the company had just completed contacting the affected active users to rest their passwords.
- **What Were The Social, Legal And Ethical Implications Of The Decisions Made:** For users whose credit or debit cards had being compromised, they opted for:
  - placing fraud alerts
  - getting free copies of their credit report (preferably several times annually, as specified by law).
- **ICO Notified:** In August 2015, an agreement called for Adobe to pay $1.1 million in legal fees and an undisclosed amount to users to settle claims of violating the Customer Records Act and unfair business practices.

DETAILS ABOUT THE BREACH CONTINUATION 3

- **Mitigation I Would Have Put:**
  - Multi-Factor Authentication,
  - Authorization, privacy controls
  - Firewall,
  - Intrusion Detection and Protection Systems,
  - Endpoint Security Software,
  - Penetration and Vulnerability testing,