Kim Ryan Joseph T. Orencia 5/22/25

CS3B

Adobe Cyber Attack

Case Summary

In October 2013, Adobe Systems Inc. was subjected to a large-scale cyberattack that attacked about 38 million active customers' personal information. The attack involved unauthorized access to Adobe's network, which resulted in the stealing of encrypted passwords, customer names, and almost 3 million credit or debit card records. Furthermore, attackers broke into source code for some Adobe products, such as Photoshop, Acrobat, and ColdFusion

Type of Crime

- Unauthorized Access: Illicit access to Adobe's security systems. Medium
- Data Breach: Illegal obtaining of sensitive financial and personal information.
- Intellectual Property Theft: Illicit access to proprietary source code.

Applicable Laws

- General Data Protection Regulation (GDPR): For EU users, the GDPR requires stringent data protection and breach notification standards. CYB Software
- Payment Card Industry Data Security Standard (PCI DSS): Adobe's processing of credit card information was governed by PCI DSS, which has regulations for the secure processing of card transactions.
- State Data Breach Notification Acts: In the US, many states have enacted legislation mandating companies to alert consumers to data breaches. Adobe was sued by several states and paid a $1 million penalty and promised to improve security measures.

Impact on Affected Individuals, Companies, and Governments

- Individuals: Users were subject to the risk of identity theft and financial fraud. Affected customers were provided with one year of free credit monitoring by Adobe.
- Companies: Other technology companies, including Facebook, informed their users about the breach, particularly about password reuse across services.
- Governments: Governments enforced fines on Adobe and required better data protection practices.

Suggested Prevention Strategies

- Using Strong Encryption: employ strong encryption techniques for password storage and sensitive information.
- Implement multi-factor authentication (MFA): make account security more robust by demanding more than one form of authentication. CYB Software
- Regular Security Audits: Carry out vulnerability scans and penetration testing to detect and fix possible vulnerabilities.
- Train Employees and Users: Offer training in best cybersecurity practices and usage of strong and distinctive passwords.
- Monitor and Respond to Threats: Install intrusion detection systems and have a strong incident response plan in place.
- Secure Source Code: Have tight access controls and encryption in place to safeguard proprietary code from unauthorized use.