Security breach essay sample

Law, Security

1. About the Case

On October 3, 2013, The Adobe Systems Incorporated in the United States of America discovered that there was a cyber-attack on their network during its regular monitoring of security check. The hackers made it through breaking in to the network and stole the sensitive and personal data of the customers which includes encrypted credit and debit card information, illegal access of customer ID’s and also source code of other various Adobe products like Adobe Acrobat and ColdFusion, ColdFusion Builder. On the companies saying that the hackers got access to the encrypted customers passwords and debit and credit card numbers too. There is also a huge loss of data occurred during this data breach which impacted immense number of people internally and externally.

2. Financial Loss

According to Adobe initially it was said that over 2. 9 million customers personal data has been breached during the cyber-attack by the hackers and is also believed to be that there is some data deletion done relating to the 2. 9 million customers who were affected by this breach. The cyber-thieves stole the customer sensitive and personal data which also includes encrypted credit card information of many customers. After a few days the company confirmed that over 38 million active users have been affected and the attackers got access to their IDs and encrypted passwords and also to many Adobe accounts which are inactive. A 3. 8 GB data was stolen from the Adobe by the attackers which includes of 152 million usernames. As a part of compromise the company is resetting the passwords for all the customers who are suspected of being attacked by the hackers, by sending them an alerting email notification which consists of the process of changing the passwords for the accounts.

The company is also offering a one year complimentary subscription to a credit-monitoring program for the US customers whose debit/credit card details are believed to be stolen. This would cost the Adobe $300 with $100 dollar per effected person and it's a huge amount to spend. Keeping it aside the cost for notifying each customer through mail letter would be around $17, 480, 000. This incident does not effected company in financially but also in reputation and business too and also could have various contrary effects later on. In this massive data breach the hackers even got the data of 234, 379 military and government accounts, encrypted passwords email addresses and passwords hints in the compromised database.

3. Status of the Case

After this massive cyber-attack incident Adobe approached the Federal law enforcement to assist them in this case and find the culprits and they are working with them. From October 2013 Ireland's Office of the Data Protection Commissioner (DPC) took over the case and are investigating to find out the hacker behind this data breach. The investigation is still under progress and are working on it to find out the culprit behind this massive data breach.

4. Steps to Avoid the Breach

The primary thing that should follow by the companies to avoid this type of incidents are, they should have a strong cyber security program and every data in there network should be encrypted and encoded. The following are the technical steps to be taken to avoid or deterred or stopped from causing the data breaches are: Each and every data should be encrypted and are maintained in privacy. Implementing the strong password is the easiest and primary way to strengthen your security. Must update the software programs regularly and make sure of updating the password in a regular manner. Frequent examination should be done and ensure that everything remains appropriate under security measure and up to date.

The following are some of the behavioral steps to be taken to avoid or deterred or stopped from causing the data breaches are: Educating the employees about the safe online surfing and make sure them understand how important is the company's data is. Be careful with the unwanted emails and spam's which makes your data vulnerable to get attacked by the hackers. Employees should obey and must follow the rules and regulations which are implied by the company. Each and every employee should not share the password with other employees even, only if insist by the supervisor.[9]

5. References:

BBC News technology http://www. bbc. co. uk/news/business-24392819 [2] ^ Digital Photography Review http://www. dpreview. com/news/2013/10/03/adobe-accounts-hacked-data-exposed-for-2-9-million-customers? ref= related-news [3] ^ Adobe Blogs http://blogs. adobe. com/security/2013/10/illegal-access-to-adobe-source-code. html [4]^Computerworld. com http://www. computerworld. com/s/article/9243010/Adobe_hack_shows_subscription_software_vendors_lucrative_targets? pageNumber= 1 [5] ^ Tripwire. com The state of Security http://www. tripwire. com/state-of-security/vulnerability-management/adobe-data-breach-compromised-234379-military-government-accounts/ [6] ^ Adobe. com http://helpx. adobe. com/x-productkb/policy-pricing/customer-alert. html/ [7] ^ Adobe. com http://helpx. adobe. com/x-productkb/policy-pricing/customer-alert. html/ [8] ^ ZDNet http://www. zdnet. com/adobe-investigated-by-data-watchdog-over-massive-security-breach-7000024973/ [9] ^ kroll cyber security http://www. krollcybersecurity. com/resources/data-security-resources/data-breach-prevention-tips. aspx