**Lab 2: *Breaches & Cyber War***

**Name: Khai Phan**

**Student Number: 100901164**

**Important Notes:**

1. The name of the document when submitted should be *<<MySeneca Username>>\_L2.docx*
2. The submission should be done through the course’s website on Blackboard

**Results**

**Part 1: Breaches**

***Breach 1*** *(Adobe Oct.3, 2013)*

**Company:** Adobe Corporation

**Method:** Unauthorized intruder has access to the web-server and then access to other server using Adobe’s network to have access to the database. Hacker took the opportunity of the alert from one of the hard drive that stored customer data and breach in.

**Data Lost (volume):** at least 38 millions users to up-to 150 millions users, source code of some software like Adobe Acrobat, Adobe Reader, Adobe Photoshop and Adobe ColdFusion

**Data Lost (types):** 3 millions credit card record, from 38 to 150 millions customer information (including username and password)

**Company Impact:** An agreement was made in 2015 that Adobe responsible for $1.1 millions in legal fee

**Customer Impact:** So far there hasn’t been a report on Customer Loss

**Remedial Action (data loss):** Adobe immediately urge customer to change their password as soon as they can (for active user) without telling the exact reason, non-active or test account password will be change by Adobe and they can reset it later.

**Remedial Action (breach):** There was no report on how exactly Adobe did to avoid any future attack. The issue could be that, when they were trying to make the back up with the hard drive, somebody took the opportunity to break in and steal the data, which is workplace integrity.

**References:**

<https://krebsonsecurity.com/2013/10/adobe-breach-impacted-at-least-38-million-users/>

<https://www.csoonline.com/article/2130877/the-biggest-data-breaches-of-the-21st-century.html>

<https://krebsonsecurity.com/2016/11/adobe-fined-1m-in-multistate-suit-over-2013-breach-no-jail-for-spamhaus-attacker/>

***Breach 2 (eBay May 22, 2014)***

**Company:** eBay Corporate

**Method:** Phishing Attack. eBay has detected some unusual behaviors in the company network using anomalies to check for data within enterprise and data transfer through enterprise

**Data Lost (volume):** 145 millions user

**Data Lost (types):** username, password, and personal information, no bank information has been lost (if the account is linked with Paypal)

**Company Impact:** There is no big harm impact, especially in payment method since most of the user have been linked with Paypal.

**Customer Impact:** Since eBay is a platform of selling and buying, beside payment information (which has been linked via Paypal as a mandatory), not much personal information has been found on most of the accounts

**Remedial Action (data loss):** eBay immediate pushing out email to tell customer change their password without telling the exact reason. They also recommend customer not to use the same old password elsewhere and if they do, eBay also urge them to change on that platform too.

**Remedial Action (breach):** eBay has confirmed it has fixed the issue but didn’t publicly tell or explain which way or which method as to avoid attacker to attack in the future.

**References:**

<https://www.mcafee.com/blogs/enterprise/cloud-security/how-bad-is-the-ebay-breach-here-are-the-stats/>

<https://www.bankinfosecurity.com/ebay-a-6858>

<https://krebsonsecurity.com/2014/05/ebay-urges-password-changes-after-breach/>

In Most of the attack, the victim never tells how they fix and improve the security issue because by doing that, they are filtered the security solution they used and attacker now can shorten the time of finding method to attack. It is, important to know that, once the attack is there, both company has acted almost immediately to solve the issue with their customer first and then solve the issue later on. Adobe even took a hand in to reset password for non-active account.

**Part 2: Cyber Security Game**

<<Insert screen capture of the completed game showing you have completed all challenges>>

