Adobe Data Breach of 2013

March 28, 2022

Submitted to: Dr. Amir Ghazinoori

Submitted by: Jasmeet Kaur (107154213)

Course Name: Security, Privacy, and Ethics for Business Analytics

Course Code and Section: BAN 220-NAA

Word Count: 1675

Time Magazine has rightly stated "Cyber war is not the future, rather it is already here". In today's digital era, as data breaches are producing headlines, enterprises are facing rising scrutiny of their anti-fraud procedures and security practices. With the great amount of significance given to technological innovation and development by tech giant Adobe, anyone would believe that the company would have an affinity for effective infrastructure to ensure data protection and security. To our disappointment, Adobe like any other mega tech company has a record of data breaches and security vulnerabilities that have permitted hackers to access the records on personal computers through Adobe Reader, get access to Adobe's security and authentication system through internal servers, generate fake updates of the Flash Player to download malicious computer software, use open back doors on an individual's computer to steal sensitive data and make malevolent PDF attachments. Although, Adobe had been proactive to address each security breach issue by providing necessary software updates and improving security infrastructure, these security violations have great impact on consumers, company, employees, and shareholders.

In 2013, Adobe experienced one of the biggest data and security breaches of the 21st century. The company formally informed about the breach on 3rd October 2013 with the announcement of the effect on 3 million people which grew to 150 million within a week of statement. Adobe's Chief Security Officer (CSO) revealed that hackers got access to most of the company's software especially Acrobat PDF and ColdFusion (web application). The hackers also stole source code of the Photoshop. The data breach uncovered usernames, email addresses, payment records and passwords of approximately 38 million people. Also, file containing information of 64,000 past and present employees of the company was also stolen[1] (BBC News). What exemplified the effect of the breach is the fact that sensitive information including credit and debit card information, contact details were stolen from Adobe's website

[1] BBC News. "Adobe Hack: At Least 38 Million Accounts Breached."

and database which reflected diverse customer base. The analysis of compromised accounts showed 234,739 records belonged to military and government, 2 million were of educational institutes, 6,000 accounts were part of defence contractors such as Raytheon. Also, 82 NSA accounts, 433 FBI accounts and 5,000 NASA records were compromised[2] (Dubey).

What makes this incident **one of the top 20 data breaches of 21st century** is the infringement of sensitive financial information of millions. Being a victim of financial information theft can lead to inconveniences like frequent modification of passwords, enacting credit freezes, supervising identity, and so on. Within a month of the data breach incident, it was clear that its repercussions were more than being stated or anticipated. Since people have practice of using same password for more than one website, many companies like Facebook had issued warnings to its users to alter their passwords and therefore the data breach made other companies also susceptible to attacks. The implications data breach can be understood through following words of Alex Holden, owner of Hold Security firm "[This breach] is one of the worst in history of the U.S. because the source code of an end user product such as Adobe Publisher and Adobe Reader was leaked and breached. This allows additional attack vectors to be discovered and viruses to be written for which there are no defenses[3] (DesJardins)"

The question that fascinates everyone is how the hackers were able to exploit the security infrastructure and vulnerabilities causing data breach in one of the mega tech-giant i.e., what caused the breach? There were several factors triggering the breach. In the five to six years prior to the data breach incident, the company faced several cyber security related problems. Adobe Reader and Adobe Flash Player held the second place as the most vulnerable programs of 500 companies in Fortune in 2009. Considering 2013 breach, Adobe technical professionals made three huge mistakes. Firstly, they used the same key for encrypting each single password.

[2] Dubey, Gaurav. "Adobe Security Breach."
[3] DesJardins, Sarah. "Cyber Attacked: Could You Be Next?

Secondly, they used an unreliable encryption technique known as ECB mode which makes it easier for criminals to crack the code. Lastly, password hints were not encrypted. The other factor contributing to the breach was transition to cloud-based SaaS (software as a service) which made security infrastructure of Adobe more vulnerable. This confirms that less focus on assuring safety of software and security of data led to exploitation of vulnerabilities. Arkin, the Adobe's CSO explained "In the old days, the idea that product engineering was totally separate from IT security did not really hold anymore"[4](Bell). Had there anything company failed to do that could have prevented the data breach incident? The answer would be affirmative as Adobe should have followed proper enforcement of industry level safety and security standards. It came to notice that one out of every six passwords were easily breakable because of hashing as encryption method which can be easily deciphered. According to Brain Kerbs, an investigating officer Adobe did not seem to put much effort to protect their customer's information by not advancing data security techniques [5].

The effect of any data breach incident is measured by proactive response and preventive measures taken by the affected company. Brad Arkin, Adobe's first CSO after breach apologized publicly and took proactive measures to minimize the potential damages. Firstly, they reset the passwords of all relevant customers like those belonging to government agencies. Secondly, accounts of customers affected by the breach were notified through emails with detailed instructions on how to reset the passwords. Lastly, for customers involving debit and credit card information violation, special services were provided to protect the account against possible abuse. These customers were presented with one-year complimentary credit monitoring services *to regain their trust*. The company also partnered with the banks and federal law enforcement to ensure protection of their customers' accounts and assist in

[4] Bell, Terena. "Adobe's CSO Talk Security, the 2013 Breach, and How He Sets Priorities.
[5] Dubey, Gaurav. "Adobe Security Breach."

investigation respectively. Also, many preventive measures were taken by Adobe by increasing their focus on improving security features to avoid such incidents from happening again. Adobe created a C-level position to enhance procedures and having a Chief Security Officer helped creating a sense of security and according to Arkin the major lesson learnt from 2013 breach is "doing a good job for security is only part of preventive actions. A part of what it means to be secure is that people must feel secure." On how their security policies and procedures changed after incident Arkin described the need to "proactively make things secure through a strategy of defense in depth," explaining that doesn't mean putting "one line of defense in place" as there exists no perfect code that is free of any possible flaws and multi-layer protection system is required to ensure network safety and data security. He also highlighted importance of response mechanism "you've got to be prepared to respond when something doesn't go right" [6](Bell). Therefore, the way 2013 data breach was handled by Adobe through proactive measures, support services and preventive actions helped company regaining customer trust, averted an adverse public reaction or outcry and avoided any similar incident till date.

Now the question is what were the consequences of security negligence for the Adobe? In terms of legal outcome, a class action lawsuit was filed in California at the federal court in November 2013. It was asserted by plaintiffs that Adobe did not conform to required industry standards to safeguard customer data. The lawsuit was settled by Adobe in 2015 by compensating $1.2 million of the legal fees of the plaintiffs. The settlement also expected Adobe to execute vigorous intrusion recognition, encryption techniques and network segmentation and to submit to an independent security audit within a year of the settlement being accepted[7] (Adobe Data Breach Class Action Lawsuit). Also, when an organization goes through an event as devastating and traumatic as a data breach, one can believe that there will

[6] Bell, Terena. "Adobe's CSO Talk Security, the 2013 Breach, and How He Sets Priorities.
[7] "Adobe Data Breach Class Action Lawsuit." *Gibbs Law Group*,

be impacts on employees which is not usually emphasized by the media and are not noticed until months later. In case of Adobe, these came in the form of lay-offs, restructurings of the company, and compulsory training sessions involving security procedures and policies.

Based on Adobe's Data Breach case study, I would recommend all stakeholders i.e., concerned organizations, the government, and individuals take steps in unison for preventing any data breach incident. Organizations must adopt latest cyber techniques in accordance with industry level security standards like the use of unique password hints as learnt from this case study. For example, use of salting technique by Adobe in addition to hashing would have been more secure way to store customer's passwords and could have averted the data breach of 2013 as decryption would have been difficult. Government should formulate laws and regulations ensuring proper compliance of safety and security standards by a company. Also, customers are also responsible to establish unique passwords by using techniques like password paraphrasing. By analysing the database after data breach, it was observed that 1.9 million of the infringed accounts had used "123456" and 211,000 accounts had used "adobe123" as their password and over 345,000 had employed the word "password"[8] (DesJardins). Having a strong password may have dissuaded hackers from trying to break into accounts.

I would conclude with the lesson that I learnt from the case of Adobe Data Breach of 2013. The safety and security of data and infrastructure of any company is only as strong as the weakest link in its security chain and sometimes "walls" protecting the data develop cracks permitting attackers the access to sensitive data. Proactive response and preventive measures in line with digital evolution define the overall affect of data breach on a company. Collective steps by organizations, individuals and government can not only prevent such incidents but can also minimize the potential harmful effect if ever they occur.

[8] DesJardins, Sarah. "Cyber Attacked: Could You Be Next?

Bibliography:

"Adobe Data Breach Class Action Lawsuit." *Gibbs Law Group*, 4 Aug. 2017, www.classlawgroup.com/adobe.

Bell, Terena. "Adobe's CSO Talk Security, the 2013 Breach, and How He Sets Priorities." *CSO Online*, 12 Apr. 2018, www.csoonline.com/article/3268035/adobe-s-cso-talks-security-the-2013-breach-and-how-he-sets-priorities.html.

BBC News. "Adobe Hack: At Least 38 Million Accounts Breached." *BBC News*, 30 Oct. 2013, www.bbc.com/news/technology-24740873.

DesJardins, Sarah. "Cyber Attacked: Could You Be Next?" *Scholars Archive, University at Albany, State University of New York,* 12-2014, www.scholarsarchive.library.albany.edu/cgi/viewcontent.cgi?article=1025&context=honorscollege_business

Dubey, Gaurav. "Adobe Security Breach." *Slideshare*, www.slideshare.net/GauravFouzdar/adobe-security-breach-30650671. Accessed 28 Mar. 2022.