Haseeb Minhas

IT 263

March1, 2021

Prof. Devaney

**EBAY BREACH 2014 TECHNOLOGY REPORT**

A leading online marketplace called eBay came into being in 1995 founded by Pierre M. Omidyar with its headquarters in San Jose, California. During the last two decades, EBay Inc. has established its position as a leading global e-commerce platform. EBay is a business to consumer as well as person-to-person online auction company it enables individuals and businesses to buy and sell products online. The working principle of eBay is a decentralized system compare to Amazon and other companies which gives more power to eBay marketplace sellers. It is a multibillionaire dollar business within over 30 countries ("Buyer Tutorial", 2016).

On **the 21st of May 2014**, eBay declared a security mishap on its data set that influenced over **148 million clients**. The size of the episode just as the quantity of clients influenced qualifies it to be the second biggest information break ever. This occurrence had presented extreme dangers for general character and secret phrase burglary as the information base containing clients' passwords had been influenced which could further damage the clients in the forms of identity theft. Concerning the break, the organization reacted by encouraging its clients to change their passwords and to utilize Visa checking administrations (McCandless, 2016). This paper examines the circumstance while dissecting how eBay took care of the security penetrate and the resultant reaction.

The rate of the security breach was fairly stunning on the grounds that the organization is one of the biggest online shops in the country. As per **eBay, the security break occurrence was accounted for to have occurred between late February and early March 2014**. By chance, programmers had figured out how to recover data from few worker subtleties and were at that point allowed admittance to eBay's information base. Following this entrance, the hacking programmers were presented **to eBay's client subtleties including their names, encoded secret phrases, and actual location, email address, DOB, and telephone numbers (Blevins, 2016).** At last, similar individuals were then ready to get to the organization's corporate organization and undermining the security of the clients' Visa data.

EBay was described as the ‘golden goose’ considering the recent exponential growth of its large user database. In the year 2014 three of the eight largest security breaches since 2005 occurred. The other attacks in 2014 comprised of the JPMorgan Chase cyber-attack and Home Depot security breach. The primary reason for such disruptive amounts of data breaches was due to an exponential increase in the amount of data stored in these companies. In fact, in 2010 the world of date total data storage was around 1.2 zettabytes but by 2015 that total increased sixth - equal to nearly 7.9 seta bytes of data this rapid growth of global data made securing private information extremely difficult and this is in part why eBay suffered such a large breach in 2014.

The breach was conducted initially through **employ hashing and salting of three eBay employees**; however, they weren’t able to access credit card credentials and similar confidential information. They did also scatter the data throughout different locations in the country they did have different data centers that held personal information and then not so personal information. Yet the breach cost Ebay decreased revenue, mostly because of its delay in announcing the mishap to its customers and as it breaches posed a serious potential risk of identity theft.

A hacker group named **Syrian Electronic Army** took responsibility for eBay’s security breach using the stolen credentials of three corporate employees… However, this information was never confirmed or investigated by eBay itself. The decline in eBay’s revenue didn’t just result from the breach itself but due to poor management of the entire scenario. The organization neglected to understand the degree of the harm until May!

Indeed, it wasn't even mindful clients' information had been influenced. "For an extensive stretch of time, we didn't accept any eBay client information was undermined," global marketplaces chief Devin Wenig said. This implies clients kept utilizing eBay for quite a long time, willfully ignorant of the malignant danger. And at the same time, the programmers continued reaping their information. Furthermore, the only compensation provided to their clients was an option and notice to **change their current passwords**; which gave rise to even more frustration as eBay servers were overwhelmed by passcode reset requests… Lastly, when three US states started examinations concerning the organization's security rehearses, eBay refused to remunerate clients or offer free credit observing.

Ways this breach could’ve been prevented were if **more attention was paid to the previous breaches** and possible steps were taken to avoid repeating similar mistakes and patterns. Another reason it was so easy for hackers to access the data was that eBay had **stored most of the stolen confidential information in plain text** and had no encryption whatsoever. Another troublesome note would be **eBay using HTTP instead of HTTPS,** as HTTPS encrypts data before sending it would have been a lot more difficult for intruders to get away with as much information as they did. Perhaps the most crucial lagging of the entire breach was, employees, lack of awareness and conscientiousness towards **spear-phishing campaign (**phishing is a type of fishing where attackers will use an email with a malicious link and it'll take you to a website that'll maybe put some malware On your computer or more often it'll have a fake login where you think it's official and you log in you put in your username and password and well it takes your username and password and saves it and sometimes it'll even just forward you straight to the actual website and log you in so you have no idea that you just logged into a fake website.) Lastly, a preventative measure could be **data scattering** through multiple serves and origins to ensure the least and incomplete data is fished if another breach is bound to occur. Currently, eBay uses **UPGUARD** to reduce potential risk and manage its security if a similar breach is bound to occur again.

I personally stay clear of any emails that require me to click links or add my login credentials. I **avoid recycling passwords,** to limit access to accounts and minimize the extent of damage in case one of my accounts gets hacked. After taking this course I have also come to an understanding of the role just **changing default passwords** can make and the differences between HTTP and HTTPS and how encryption plays a role in securing our sensitive information. Previously I have never been mindful of the consequences of data breaches on the web and how I could play my part in ensuring my data was as safe as possible. Normally I would never find myself skipping over to the data securing and risk management policy of a company that I am acquainted with; however, now I cannot bring myself to be satisfied without understanding it. Having known the potential threats it possesses to just have a PayPal account per se.

REFERENCES

1. <https://www.youtube.com/watch?v=cSPr1FHLoEo>
2. <https://www.eecs.yorku.ca/course_archive/2014-15/W/3482/Team3_presentation.pdf>
3. <https://hostingtribunal.com/blog/biggest-data-breach-statistics/>
4. <https://www.upguard.com/security-report/ebay>
5. <https://www.bbc.com/news/technology-27539799>
6. <https://ebay.q4cdn.com/610426115/files/doc_financials/financials/2015/2016-proxy-statement.pdf>
7. <https://www.essaytyping.com/security-breach-ebay/>
8. <https://www.businessinsider.com/cyber-thieves-took-data-on-145-million-ebay-customers-by-hacking-3-corporate-employees-2014-5>
9. <https://www.businessinsider.com/r-exclusive-ebay-did-not-initially-realize-customer-data-compromised-in-breach---executive-2014-23>
10. <https://www.forbes.com/sites/ryanmac/2014/05/23/as-ebay-notifies-users-of-hack-states-launch-investigation/?sh=258a8c8c6f27>