TEXAS COLLEGE OF MANAGEMENT &



INFORMATION TECHNOLOGY

**Submitted by: Submitted to:**

Name= Aanya Yadav Mr. Rajkumar Giri

Semester= 4th

Section= D

LCID= LC00017001724

**1. The Yahoo data breach of 2013-2014 was one of the largest and most damaging Cybersecurity incidents in history. The breach, which occurred in two separate incidents, compromised the personal information of over 3 billion Yahoo users worldwide. The first breach, which took place in 2013, impacted 1 billion user accounts, while the second breach, occurring in 2014, affected 500 million accounts. The breaches exposed a vast amount of sensitive information, including users' names, email addresses, dates of birth, and telephone numbers. While most passwords were hashed using the bcrypt algorithm, some passwords were protected using weaker methods, leaving them susceptible to exploitation. The attackers behind the breaches were sophisticated state-sponsored actors, believed to have been working on behalf of a foreign government. These attackers exploited vulnerabilities in Yahoo's system, particularly in the way the company handled user identifying and authorizing cookies. By manipulating these cookies, the attackers were able to assume the identities of legitimate users and gain unauthorized access to their accounts. The breaches were not discovered until years later, when Yahoo was in the process of being acquired by Verizon. This delay in detection allowed the attackers to access and exfiltrate a significant amount of sensitive information, compromising the privacy and security of millions of users. In addition to exposing sensitive user information, the breaches also had significant financial implications for Yahoo. The breaches ultimately cost the company an estimated $350 million of the sale price to Verizon, who had acquired Yahoo's core Internet business. The breaches also had a lasting impact on Yahoo's reputation, leading to a decline in user trust and confidence. The breaches served as a stark reminder of the importance of robust Cybersecurity measures and proactive security practices in protecting sensitive information in today's digital age The settlement amount for individuals affected by the Yahoo data breaches of 2013-2014 was $117.5 million. This settlement fund was intended to compensate affected individuals for losses related to the breaches, such as identity theft, delayed tax refunds, and other expenses. The actual amount received by each individual varied based on various factors, including the number of valid claims filed and the severity of the impact experienced by each claimant. As estimated, $25000 is maximum for a individual if their critical data were exposed and many peoples are claiming for the $100 as per their data loss. On March 15, 2017, the FBI accused four men of being involved in the 2014 Yahoo data breach. Two of them worked for Russia's Federal Security Service (FSB). The FBI said the actions of these men, who were part of an FSB unit that works with the FBI on Cybercrime, were very serious. The four men are Alexsey Belan, a hacker on the FBI's most wanted list, FSB agents Dmitry Dokuchaev and Igor Sushchin, who the FBI said paid Belan and other hackers to carry out the breach, and Canadian hacker Karim Baratov. The FBI claimed Baratov was paid by Dokuchaev and Sushchin to use data from the Yahoo breaches to hack into about 80 accounts not belonging to Yahoo. Baratov, the only one arrested, was sent to the United States. He initially pleaded not guilty but later admitted to hacking into at least 80 email accounts for Russian contacts. He was sentenced to five years in prison, ordered to pay $2.25 million in restitution to his victims, and charged with nine counts of hacking. The Yahoo data breach revealed several defects in Yahoo's Cybersecurity practices and infrastructure. One major weakness was the company's failure to promptly detect and respond to the breaches. The breaches occurred over a period of several years, yet they went undetected until years later, when Yahoo was in the process of being acquired by Verizon. This delay in detection allowed the attackers to access and ex-filtrate a significant amount of sensitive information, compromising the privacy and security of millions of users. Another flaw exposed by the breaches was Yahoo's inadequate encryption and password protection practices. While most passwords were hashed using the bcrypt algorithm, a more secure method, some passwords were protected using weaker methods, leaving them vulnerable to exploitation. This failure to properly protect user passwords and other sensitive information was a critical oversight that allowed the attackers to access and compromise a vast amount of user data. Furthermore, the breaches highlighted Yahoo's lack of robust incident response capabilities. Following the discovery of the breaches, Yahoo took several steps to improve its security posture, including implementing stronger encryption and password protection measures. However, these measures were seen by many as reactive rather than proactive, indicating a lack of comprehensive incident response planning and execution. In response to the breaches, Yahoo implemented several measures to improve its security posture and protect user data. The company introduced stronger encryption and password protection measures, as well as enhanced authentication methods, to prevent future breaches. Yahoo also bolstered its incident response capabilities, conducting regular security audits and providing employee training on Cybersecurity best practices. Despite these efforts, the breaches had a lasting effect on Yahoo's legacy and reputation. The breaches served as a cautionary tale for other organizations about the dangers of complacency in the face of evolving Cyber threats. The breaches also highlighted the need for organizations to prioritize Cybersecurity and implement robust security measures to protect user data. Overall, the Yahoo data breach of 2013-2014 was a watershed moment in the history of Cybersecurity, underscoring the importance of vigilance and proactive security practices in protecting sensitive information in today's digital age. Questions:**

**a) How did the attackers exploit vulnerabilities in Yahoo's system to carry out the data breaches of 2013-2014? Describe the methods used and the specific weaknesses in Yahoo's Cybersecurity practices that were targeted. (5)**

**b) What actions did Yahoo take to enhance its security posture and prevent future breaches following the 2013-2014 incidents? Discuss the implementation of stronger encryption, password protection measures, and incident response planning. (5)**

**c) Why did it take Yahoo several years to detect the data breaches of 2013-2014? Discuss the factors that contributed to the delayed detection and the consequences of this delay. (5)**

**d) Were the attackers behind the Yahoo data breaches identified, and what legal actions were taken against them? Describe any charges, lawsuits, fines, or imprisonment sentences imposed on the individuals involved. (5)**

**e) What were some of the broader implications of the Yahoo data breaches of 2013-2014 for the Cybersecurity landscape and the protection of user data online? Discuss how these breaches influenced security practices and regulations in the tech industry. (5)**

**Ans:**

**a.** The primary method used by the attackers to take advantage of Yahoo's system vulnerabilities was to manipulate user identity and authorization cookies. The attackers were able to assume the identity of authentic users and obtain unapproved access to their accounts thanks to these cookies. Without knowing user passwords, the attackers were able to take over user accounts by taking advantage of flaws in Yahoo's handling of these cookies. Bypassing conventional authentication procedures, this technique gave the attackers access to private data.

Targeted were certain shortcomings in Yahoo's cybersecurity procedures, such as:

i. Insufficient cookie handling: Because Yahoo's system was not set up to safeguard or validate user cookies, attackers were able to modify them and obtain unauthorized access.

ii. Insufficiently strong authentication methods: Yahoo mostly used cookies to authenticate users instead of implementing extra security measures like two-factor authentication (2FA).

ii. Delayed detection: The harm on users was exacerbated by Yahoo's inability to identify the breaches in a timely manner, which allowed the attackers to maintain their unlawful access for several years.

**b.** Yahoo implemented a number of measures to strengthen its security posture and avert such vulnerabilities in the future after the 2013–2014 attacks:

i. Implementation of more robust encryption: Yahoo implemented the bcrypt algorithm for password hashing, among other more robust encryption techniques, to better safeguard sensitive user data.

ii. Yahoo strengthened their password security procedures, making sure that the majority of passwords were hashed using safe techniques to thwart unwanted access.

iii. Enhanced incident response planning: To better identify and address security breaches, Yahoo strengthened its incident response capabilities by implementing thorough incident response plans, conducting frequent security audits, and training staff members on cybersecurity best practices.

These steps were intended to bolster Yahoo's overall cybersecurity defenses while addressing the specific vulnerabilities that the attackers had exploited.

**c.** Yahoo took several years to discover the 2013–2014 data breaches because of a number of circumstances, including:

i. Absence of proactive monitoring: Yahoo lacked strong measures to immediately identify questionable activities or unlawful access to user accounts.

ii. Complexity of the Attacks: Yahoo's security staff had a difficult time identifying the breaches since the attackers used complex ways to take advantage of several vulnerabilities.

iii. Prioritize other matters: Yahoo might have been more concerned with other facets of its operations, like acquisitions and mergers, which took time and money away from cybersecurity.

Millions of users' security and privacy were jeopardized as a result of this delayed detection, which gave the attackers access to and exfiltrated a substantial amount of sensitive data.

**d.** Yes, legal action was taken against the attackers responsible for the Yahoo data breaches after they were identified. Two FSB agents and two hackers were among the four people the FBI accused of being engaged in the hacks. One of the hackers, Alexsey Belan, was on the FBI's most wanted list. The only person detained was the Canadian hacker Karim Baratov, who received a five-year prison term. He was forced to make amends to his victims after admitting to breaking into Russian contacts' email accounts.

e. The Yahoo data breaches that occurred between 2013 and 2014 have wider effects on internet user data privacy and cybersecurity:

i. A greater understanding of the possible dangers of insufficient security measures was brought about by the breaches, which also emphasized the significance of strong cybersecurity policies.

ii. Stricter rules and compliance criteria were introduced as a result of regulatory authorities' increased scrutiny of internet companies' cybersecurity activities following the hacks.

iii. Trust and reputation: The hacks seriously damaged Yahoo's standing and reduced user confidence, underscoring the significance of preserving user confidence via strong cybersecurity protocols.

iv. Changes across the industry: The hacks had an impact on security procedures throughout the tech sector, motivating businesses to give cybersecurity top priority and bolster security protocols in order to safeguard user information.

**THANK YOU**