Report on Yahoo Data Breaches

Prepared by: Akhil Reddy Gattu AND Hrithik

This report provides an analysis of the Yahoo data breaches that occurred between 2013 and 2016. The breaches compromised billions of user accounts and had significant repercussions. We will address several key questions regarding the security properties violated, the victim population, technological/organizational weaknesses, and threat vectors employed by the attackers.

Security/Privacy Property Violated	**Consequence(s)**	**PII**	**Evidence in Report on Yahoo Data Breaches**
Confidentiality	exposed user account information, including emails and hashed passwords	Yes	The breaches exposed user data, including "email addresses, telephone numbers, hashed passwords, and, in some cases, encrypted or unencrypted security questions and answers." (Wikipedia)
Integrity	Unauthorized access to user accounts and data manipulation	Yes	Some accounts were accessed without authorization, and there were concerns about data integrity.
Availability	Yahoo services impacted during investigation		The availability of Yahoo services might have been affected during the investigations and remediation processes.

With 3 billion Yahoo users worldwide, the victim population of the Yahoo data breaches was substantial. There was no particular target demographic, area of specialization, industry, or company that was chosen as the main target. Instead, Yahoo's user base was significantly impacted by the thefts.

Technological/Organizational Weaknesses:

Inadequate Security Practices: Yahoo's security procedures came under fire for being inadequate. The level of encryption was inadequate, and it looked that security flaws weren't being patched.
Delayed Detection: The delayed identification of the intrusions constituted a serious flaw. The fact that Yahoo was unaware of the breaches until they were made public shows a deficiency in monitoring and intrusion detection.
Data Encryption: Security questions and answers and other sensitive information were not always encrypted, making them exposed.

Threat Vectors:

Stolen Credentials: The most likely way that attackers gained access was through stolen credentials was through phishing or earlier data breaches.
Exploits: System flaws might have been exploited to get access to Yahoo's infrastructure.
State-Sponsored or APT Attacks: Given the possibility of state-sponsored involvement, advanced strategies and persistent threats (APTs) may be employed.

REFERENCE:

Yahoo! data breaches - Wikipedia. (2017, December 1). Yahoo! Data Breaches - Wikipedia. https://en.wikipedia.org/wiki/Yahoo!_data_breaches

Perlroth, N. (2017, October 3). All 3 billion Yahoo accounts were affected by 2013 attack. *The New York Times*. https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html