# Analysis of Security Breach:

On surfing the internet for top security breaches that happened in 2023, a serious breach information caught my attention. One of the largest tech retailers in India – Poorvika Mobiles has been a victim to a massive data breach exposing over 8 million documents of private and customer data. The publicly exposed documents included highly sensitive personally identifiable information (PII) as well as salary information, detailed employment records, and customer data.

### Who:

According to Website Planet, a security researcher Jeremiah Fowler discovered and reported this issue as a responsible disclosure to the company. Although, this is a security practice done by an ethical security researcher with no harmful intentions, he mentioned that millions of user data were accessible to any one with an internet connection. These conditions are vulnerable to malicious attackers out there, who can make use of the available PII and exploit using phishing, ransomware and several other techniques.

### Where:

The Researcher claimed he had access to the company's database, highlighting it as non-password protected database and the file names were in a clear text format.

### What:

The database records contained employee data such as religion, sex, date of birth, marital status, family dependents, and other Personally identifiable Information such as Biometrics and Aadhar. The records also indicated employee status, designation, salary information and the reason for their departure (e.g., personal problems or health and medical reasons.

## Risk Involved:

### Customer data:

These data can be used for identity theft, targeting customers into fishing scams which leads to access of more sensitive information like passwords and credit card details.

### Employee data:

Access to employee mail id's can be manipulated for social engineering attacks by fraudsters to target specific employees to gain access to company's sensitive information.

## Risk Mitigation:

### Access Control:

- Highly sensitive data must be categorised and restrict access for authorised personnel.
- Ensure strong authentication techniques like MFA and password requirements.

- Regular security audits to ensure security and to meet security standard requirements.

## Encryption:

- Ensure data encryption for the data collected, stored and in transit using Hash methodologies like SHA 256 for stronger encryption.
- Migrating database storage to cloud solutions like Azure and AWS could benefit service availability and data integrity.