Case Study: Capitol One Data Breach (July 2019)

In July 2019, **Capitol One**, a major online banking and credit card company, discovered that its data had been compromised.

- Hundreds of thousands of **credit card applications** were stolen.
- The stolen data included **personal information**, such as names, addresses, dates of birth, and social security numbers.

Key Details

- **Unusual characteristics**:
    - The stolen data did not appear on the dark web.
    - There was no sign of industrial espionage or attacks from competitors.
- **Perpetrator**:
    - The attack was carried out by **Paige Thompson**, also known online as **Erratic**.
    - Thompson had **previously worked for Amazon**, giving her insight into cloud systems.
- **Method of attack**:
    - She identified that **Capitol One's AWS server was misconfigured** and vulnerable.
    - The breach exploited this misconfiguration to access sensitive data.
- **Motivation and outcome**:
    - The attack appeared similar to a **white-hat test**, but Thompson did not attempt to profit from the stolen data.
    - She posted a list of breached directories on her **GitHub page**, which led to her arrest.
    - No clear explanation for the attack was ever provided.

Analysis

Cause of breach

- Misconfigured **cloud server settings** allowed unauthorised access.
- Lack of proper monitoring and access controls on AWS contributed to the vulnerability.

Detection

The breach was discovered when the perpetrator made her actions public via GitHub.

Impact

- Exposure of sensitive personal information of customers.
- Potential reputational damage to Capitol One.
- Legal and regulatory scrutiny regarding data protection practices.

Lessons Learned:

1. **Cloud security is critical**: Misconfigurations can create serious vulnerabilities.
2. **Access control and monitoring** must be enforced on cloud systems.
3. **Internal knowledge can be misused**: Former employees may have insights into system weaknesses.
4. **White-hat intentions are not guaranteed**: Even if no profit is sought, personal data can be exposed and misused.
5. **Prompt detection and reporting** are essential to limit damage.