TESLA DATA BREACH

UNDERSTANDING DATA BREACHES

- A data breach is an incident where sensitive information is accessed and disclosed without authorization.
- Data breaches can involve a variety of information, including customer data, employee data, and intellectual property.
- They can have significant financial and reputational consequences for businesses.

THE BREACH REVEALED

01

- In May 2023, German newspaper Handelsblatt reported acquiring a massive dataset – the "Tesla Files" – containing confidential Tesla information.

02

- This data breach impacted over 75,000 individuals, including current and former employees.

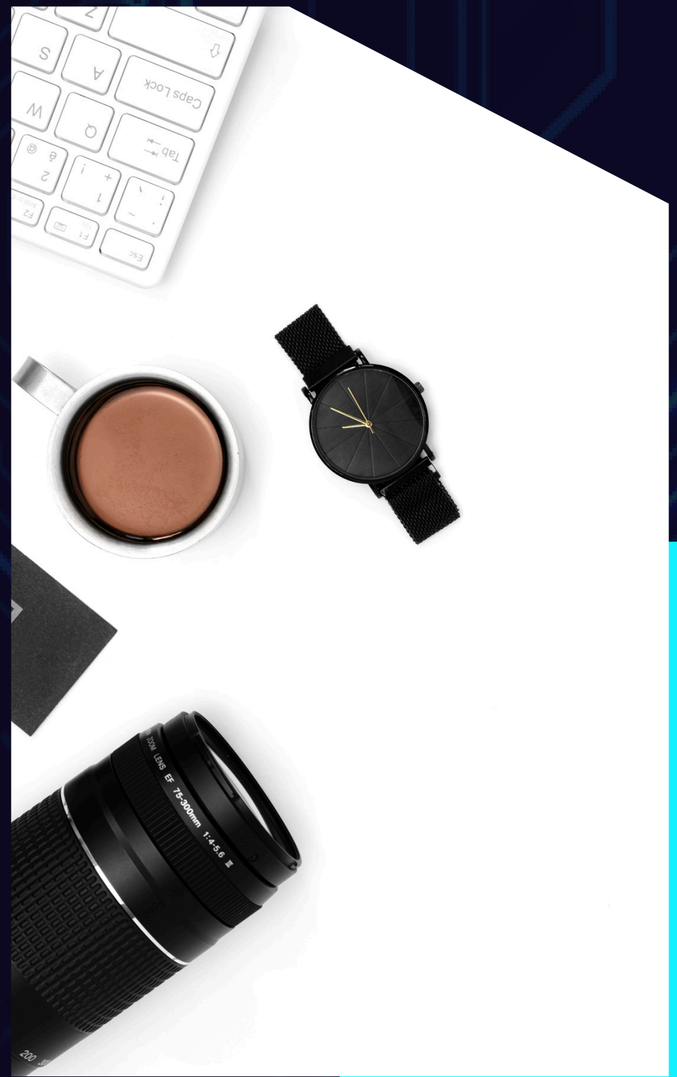
03

- Initially, a cyberattack was suspected, but investigations revealed a different story.

INSIDER CULPRIT

- Tesla's investigation identified two former employees as the culprits behind the data leak.
- These individuals allegedly breached company policies and misappropriated sensitive information.
- The data leak reportedly included employee names, addresses, Social Security numbers, and even customer bank details.



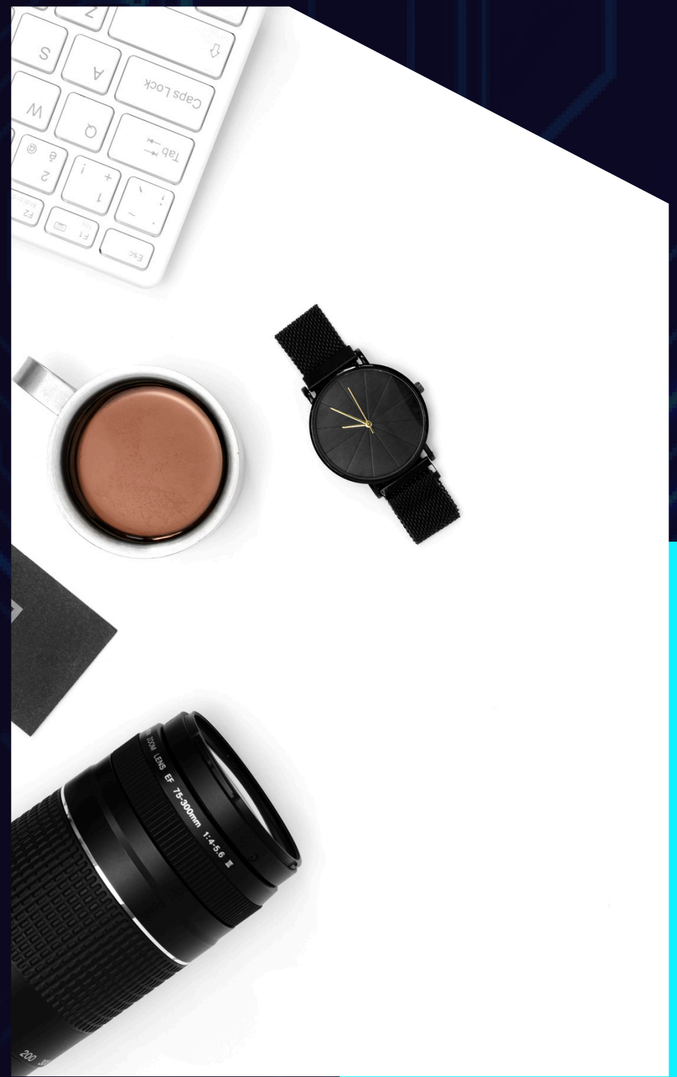


THE "TESLA FILES"

- The leaked data, dubbed the "Tesla Files," comprised a massive 100 gigabytes of confidential information.
- This data reportedly included:
  - Employee records (current and former)
  - Production secrets
  - Customer complaints about Tesla's Full Self-Driving (FSD) features
  - Potentially customer bank details

IMPACT AND AFTERMATH

- The data breach exposed sensitive information, potentially putting individuals at risk of identity theft and financial fraud.
- Tesla faced lawsuits from affected employees and investigations from data protection authorities.
- The company took steps to strengthen its data security measures and offered credit monitoring services to impacted individuals.



WHAT TESLA DID

- Tesla launched an investigation to identify the culprits and understand the scope of the breach.
- The company notified affected individuals and offered credit monitoring services.
- Tesla has taken steps to strengthen its data security protocols to prevent similar incidents in the future.

TOOLS USED IN THE INVESTIGATION

- Digital Forensics:
  - Used to identify the source of the data leak.
  - Tools like forensic software can recover deleted files and analyze system logs to reconstruct events.
- Data Loss Prevention (DLP):
  - May have helped identify suspicious data exfiltration attempts in real-time.
  - DLP solutions monitor data movement and can flag unusual activity.
- Incident Response:
  - A structured approach to contain the breach and mitigate damage.
  - Includes isolating compromised systems, securing data, and notifying authorities.

LESSONS LEARNED

- The Tesla data breach highlights the importance of robust data security measures.
- Companies should:
- Implement strong access controls
- Regularly train employees on data security best practices
- Have clear data breach response plans

THANK YOU

LOKESH SHARMA (RA2111030010151)