Here's a detailed guide for structuring your report on a real-world information security breach, specifically focusing on the **Facebook (Meta) Data Breach** that occurred in **2019**.Retrieved from www.ftc.gov --- This structure provides a comprehensive analysis of the Facebook data breach, including a detailed incident summary, impact analysis, recommended countermeasures, and conclusions.**March 2019: Discovery of the Breach:** - In **March 2019**, **security researcher** **Anurag Sen** discovered that Facebook had inadvertently exposed **user data** on **Amazon Web Services (AWS)** servers due to a misconfigured **Facebook API**.The breach resulted from a misconfigured **Facebook API** that allowed unauthorized access to databases hosted on Amazon Web Services (AWS).The breach occurred because **Facebook's API endpoints** had **improper access controls**, allowing third parties to retrieve user information without authorization.- Facebook also had to overhaul its **third-party app review process** to prevent developers from requesting excessive user information, requiring changes in operational procedures.To mitigate the risk of similar breaches, organizations must prioritize **API security**, enforce **data encryption**, and continuously monitor for **misconfigurations** in cloud environments.#### **Reputational Damage:** - The breach significantly damaged Facebook's **reputation**, especially as the company had already been under scrutiny due to previous privacy scandals (e.g., Cambridge Analytica).#### **Operational Impact:** - Facebook had to dedicate significant resources to investigating the breach, conducting **security audits**, and implementing new security measures.- Conduct **security audits** to ensure that all third-party developers and applications comply with security best practices and handle user data responsibly.Facebook, one of the largest social media platforms, faced a breach that exposed vast amounts of personal data, including phone numbers, user IDs, and other account details.- The data included **user phone numbers**, **user IDs**, **account names**, **birth dates**, and **location data**, which were all stored in **unprotected** and **publicly accessible databases**.**Type of Breach and Exposure:** - The exposed data was related to **Facebook users** who had linked their accounts to third-party applications, like mobile apps, which often request phone numbers and other personal data.It was not a malicious cyberattack but resulted from inadequate security controls over user data stored in cloud infrastructure.#### **Data Stolen:** - The exposed data included: - **Phone numbers** - **User IDs** - **Account names** - **Birthdates** - **Location data** - **Other personal details associated with users** who had linked their phone numbers to third-party apps.- The company also incurred substantial costs in **addressing the breach**, including **security upgrades**, legal fees, and the cost of dealing with **lawsuits** filed by affected users.#### **Legal Consequences:** - Facebook was subjected to numerous **lawsuits** from affected users who sought compensation for the exposure of their sensitive information.**Cloud Security Monitoring:** - Tools like **Amazon Macie** and **CloudTrail** can be used to monitor cloud environments for **misconfigurations** and unauthorized access attempts.--- ### **Conclusion:** The **Facebook data breach** of 2019 underscores the critical importance of securing APIs and properly configuring cloud infrastructure.This example is widely recognized and has had significant impacts, providing valuable insights into how breaches can occur and their consequences.--- ### **Title Page:** - **Group Details**: [Insert Group Name and Members] - **Course**: Information Security

Management – **Section**: [Insert Section] – **Date**: [Insert Date] – **Teacher's Name**: [Insert Teacher's Name] --- ### **Introduction**: In **2019**, **Facebook (now Meta)** was involved in a **massive data breach** that affected nearly **540 million users** worldwide.**June 2019: Public Acknowledgment:** – Facebook issued a public statement acknowledging the breach and apologizing to its users.– The company **reviewed and reconfigured its APIs**, ensuring that stricter access controls were implemented.– Facebook initiated a **security audit** of its data-sharing practices with third-party developers to identify and eliminate any other potential vulnerabilities.In **2019**, Facebook paid a **$5 billion fine** as part of a settlement with the **Federal Trade Commission (FTC)** related to privacy violations, which included aspects of this data exposure incident.**API Security:** – Implement **API Gateways** like **AWS API Gateway** or **Apigee** to control and monitor API traffic effectively.Retrieved from www.cnn.com 2.--- ### **References**: 1.2.3.4.5.2.3.4.