**Investigation of a Data Breach:**

**Objective:** **Investigation of a Data Breach on a Renowned Website**

Scenario: Imagine that there has been a data breach at a renowned website, and your task is to investigate this breach. While the website's name is fictional, the scenario will test your investigative and forensic skills.

Details: Company Name: ABC SecureBank, a highly reputable financial institution. Breach Discovery: The breach was discovered during a routine security audit, and it appears that sensitive customer data may have been exposed. Scope of Breach: The breach involves potential exposure of customer account information, including names, account numbers, and transaction history.

Tasks:

1. Incident Analysis:

Incident analysis helps in identifying patterns and trends within a system. Customer data has been leaked including names, account numbers, and transaction history. Hence, they can get also the account numbers where the money has been transferred. Through this exposure hackers can easily hack their accounts and email ids can be also hacked to get the link they have with other accounts. Thus, all these customer data are in high risk. The security system should has been more protected and once the attackers have attacked an alert should have passed.

1. Forensic Analysis:

Different forensic tools are used to do Forensic Analysis. Unauthorized access has been identified and further investigating evidences have been kept. Back door programs detected and are taken care of. All the IP(s) actively working at that time are been kept and monitored to detect any flaw.

1. Data Recovery:

Data recovery is a process of retrieving deleted, inaccessible, lost, corrupted, damaged, or formatted data from secondary storage, removable media or files, when the data stored in them cannot be accessed in a usual way.

1. Regulatory Compliance:

All the laws to be taken care while investigating the breach. Rules and regulations must be followed.

1. Communication and Notification:

Communication among the staffs should have been better to avoid such circumstances. Notification and alerts should have been there to take care of the situation at the required time.

1. Post-Incident Review:

Confidential informations leaked of many people and their personal data are at high risk. Anytime any hacker can hack their systems. They are at high alerts.