Case Study: Equifax Data Breach

Equifax, one of the biggest credit reporting agencies, experienced a major data breach in 2017. Hackers gained access to the personal information of 147 million people due to a failure to patch a known software vulnerability. This incident put millions of people at risk of identity theft. Below is a response plan that would help prevent or manage a similar situation in the future.

Incident Response Plan

1. **Detection Method: Using SIEM Systems**
   The first step is **detecting any unusual behavior on the network**. A **Security Information and Event Management (SIEM)** system helps with this by keeping an eye on all network activities and sending alerts for strange behavior, such as multiple failed login attempts. Some examples of SIEM tools are **Splunk, IBM QRadar, and SolarWinds**. They help companies stay on top of potential threats in real-time.
   In Equifax's case, a SIEM could have noticed unusual access patterns that pointed to a security problem. Alongside a SIEM, an **Intrusion Detection System (IDS)** like **Snort or Suricata** can help catch suspicious activities, like unauthorized access or malware.

2. **Containment Strategy: Disconnect Affected Systems**
   If a security problem is detected, the next step is **containing the threat** by quickly disconnecting any affected systems. This keeps the issue from spreading to other parts of the network. Companies should also **segment their networks** to limit access to sensitive areas. For instance, Equifax could have restricted access to Social Security numbers, making it harder for hackers to access everything at once.
   Using **firewall rules** and **Access Control Lists (ACLs)** can also help by limiting who and what can access different parts of the network. Blocking suspicious IP addresses, disabling compromised accounts, and securing backup systems are other effective containment measures.

3. **Eradication Steps: Remove the Root Cause**
   Eradication means **finding the cause of the problem and removing it**. For Equifax, the cause was an unpatched vulnerability in their software. Running regular checks on the network using a **Vulnerability Management Program (VMP)** can help detect weaknesses before hackers find them. Tools like **Qualys, Nessus, and Rapid7** scan for vulnerabilities and help security teams fix them.
   Once the cause is identified, any malicious software should be removed, passwords reset, and systems checked to make sure no hidden threats remain. Regular checks after fixing an issue help ensure the problem doesn't return.

4. **Recovery Steps: Safely Restoring Systems**
   Recovery involves bringing systems back online carefully after fixing the issue. This could include restoring from clean backups and double-checking all updates are applied. In Equifax's case, recovery would be done in stages to make sure there are no remaining threats. Tools like **endpoint detection and response (EDR)** can monitor systems in real-time to catch any suspicious activity.

5. **Cyber Attack Explanation: Ransomware**
   Ransomware is a type of attack where software locks files and demands a payment to unlock them. It usually spreads through phishing emails or exploiting weak security. A ransomware attack could have worsened Equifax's breach by making the data inaccessible without paying a ransom. To prevent this, employees need training to recognize phishing and companies should maintain regular backups.

Comprehensive Security Policy

1. **Key Security Rules/Guidelines**:
   - **Use Strong Passwords**: Passwords should be complex and changed regularly to reduce unauthorized access risk. Using a

password manager helps create and store strong passwords.

- **Enable Multi-Factor Authentication (MFA)**: MFA adds a second step to logins, like entering a code sent to your phone. It adds an extra layer of protection, especially for sensitive data.
- **Keep Software Updated**: Regularly updating software patches security gaps. Equifax's failure to update its software led to the breach. Using automatic updates can help prevent this kind of vulnerability.

2. **Incident Response Steps**:
    - **Document Actions**: Keep track of all actions taken during a breach. This includes recording when the breach was discovered, what actions were taken, and which systems were affected.
    - **Notify Key Teams**: Alert IT and management immediately, and, if needed, bring in external cybersecurity experts to help control the situation.

3. **CIA Triad Maintenance**:
    - **Confidentiality**: Ensures that only authorized users can see sensitive data. For example, using **data encryption** and **role-based access control (RBAC)** restricts access to certain users.
    - **Integrity**: Makes sure data remains accurate and isn't changed without permission. **File integrity monitoring (FIM)** tools can detect unauthorized changes.
    - **Availability**: Ensures systems and data are available to authorized users when needed. Equifax could ensure this with **disaster recovery plans** and regular backups.

Encryption Techniques

1. **Encryption Example**:
    - **Encrypted Text**: With AES-256 encryption, a message like `This is a secret message.` becomes a string of random characters like `U2FsdGVkX1+7h3F0g4k4kkYHq...`. Without the decryption key, the message can't be read.
    - **Decrypted Plain Text**: Once decrypted, the original message is readable again as `This is a secret message.` This process ensures that data stays secure even if it's intercepted.
    - **Hashed Text**: Hashing creates a secure code from data. Using **SHA-256** to hash a password like "Password123" might turn it into `ef92b778...`. Hashing is one-way, meaning it can't be reversed back to the original data, making it useful for protecting passwords.

Encryption and hashing help protect data from unauthorized access. Even if data is stolen, it's unreadable without the correct key or hashing method.

-

Legal and Ethical Compliance

1. Laws/Regulations:

- General Data Protection Regulation (GDPR): A European law that requires companies to protect personal data and report breaches quickly. Equifax would have had to inform European customers of the breach within 72 hours and explain the impact on their data.

- Health Insurance Portability and Accountability Act (HIPAA): A U.S. law that protects health data. While not specific to Equifax, HIPAA is an example of strict data protection rules that apply to sensitive information,

requiring secure storage and quick response to breaches.

2. **Ethical Consideration:**
    - Being transparent with customers about data usage and breaches is an ethical responsibility. Notifying affected people builds trust and shows the company is accountable. Even if not required by law, companies should prioritize honesty.

3. **Compliance Explanation:**
    - An effective response plan aligns with laws like GDPR and HIPAA to ensure proper handling of data and quick breach notifications. Equifax's delay in reporting the breach led to legal and reputational issues. Following a compliance-focused plan helps protect customer data and the company's reputation.