Case Study: *Equifax Data Breach*

Incident Response Plan

- **Detection Method:** Detection Method: Use a Security Information and Event Management (SIEM) system that watches for unusual activity on your network. It alerts you if something strange happens, like too many failed login attempts.

    - **Containment Strategy**: If you spot a security problem, quickly disconnect the affected computers from the internet and the company network. This helps stop the problem from spreading.
    - **Eradication Steps**: Find out what caused the issue, remove any harmful software, and fix any weaknesses in your systems.
    - **Recovery Steps**: Carefully bring the systems back online and make sure everything is up to date. Keep an eye on them for any new problems.
    - **Cyber Attack Explanation**: **Ransomware** is software that locks your files and asks for money to unlock them. It usually comes from phishing emails or weak security.

Comprehensive Security Policy

- **Key Security Rules/Guidelines**:
    - **Use strong passwords**: Make passwords long and mix letters, numbers, and symbols. Change them regularly.
    - **Use multi-factor authentication (MFA)**: This means you need a second step to log in, like a code sent to your phone.
    - **Keep software updated**: Regularly install updates for all your programs to fix security holes.
- **Incident Response Steps**: If there's a breach, follow the steps in your incident response plan, like alerting the IT team and keeping a record of what happened.
- **CIA Triad Maintenance**:
    - **Confidentiality**: Make sure only allowed people can see sensitive data.

    - **Integrity**: Check that data is correct and hasn't been changed without permission.
    - **Availability**: Ensure data and systems are usable, even if something goes wrong.

Encryption Techniques

- **Example**:
    - **Encrypted Text**: Using AES, an example encrypted message could look like `U2FsdGVkX1+7h3F0g4k4kkYHq...`, making it unreadable.
    - **Decrypted Plain Text**: After decrypting, the original message would be `This is a secret message.` showing it can be read again.
    - **Hashed Text**: Use SHA-256 to change "Password123" into a secure code like `ef92b778...`. Hashing keeps passwords safe since you can't turn it back into the original text.

Legal and Ethical Compliance

- **Laws/Regulations**:
    1. **GDPR**: A law in Europe that protects people's data and requires companies to handle it carefully.
    2. **HIPAA**: A U.S. law that protects patient health information and requires secure handling.
- **Ethical Consideration**: Be honest about how you use data. If there's a breach, let people know right away to keep their trust.
- **Compliance Explanation**: The plan should show how it follows laws like GDPR and HIPAA, ensuring personal data is safe and users are informed quickly if there's a problem.