Project_Overhaul_Oscorp_Current_State

Current Oscorp Cyber Security Team:

- Cyber Security Analyst – Generalist. Responds to cyber incidents as they come. Reports to Oscorp's IT manaer.
- Network engineer - Manages the firewalls. Reports to the Network Team Leader.
- Cyber Security Consultant - My new role at Oscorp. I will initially report to the IT Manager.

Oscorp Current Cyber Security Controls:

- **Organizational Governance:**
    - The CEO has a clear business strategy for the business. However, roles and responsibilities for cyber security have not been defined. They are assigned to the IT team. There is no clear cyber security strategy.
- **Asset Management:**
    - The IT team has a spreadsheet with serial numbers of laptops.
      The spreadsheet includes the model of each machine and details about the warranty.
    - Oscorp uses Microsoft Office365 and relies exclusively on Software-as-a-Service applications.
    - All data is in Microsoft Azure cloud.
    - The IT team uses a Secure Operating Environment (SOE) to image all their laptops with the latest Windows desktop version.
- **Business Continuity and Disaster Recovery:**
    - The IT team conducts regular disaster recovery testing.
    - The IT team has clear and documented business continuity plans.
    - The IT team takes regular backups.
    - Backups are assessed periodically.
- **Vulnerability Management:**
    - Oscorp has purchased a Qualys vulnerability scanner.
    - The IT team uses Qualys on an ad-hoc basis.
    - There is no formal vulnerability management program in place.
    - A large number of high and severe vulnerabilities have been reported by Qualys.
- **Risk Management:**

- Oscorp has a risk team that performs financial risk activities.
- There is no technology or cyber risk process at Oscorp.

- **Third Party Risk Management (TPRM):**
  - Oscorp does not perform any third-party risk management.
  - Contracts are reviewed by the Procurement and Finance departments, not the IT department.

- **Identity and Access Management (IAM):**
  - Oscorp uses Microsoft Active Directory to manage users and groups.
  - There is no privileged access management solution in place.
  - Admin account password is shared with a few senior members of the IT team.
  - Access to resources is granted upon request.
  - The organization does not use two-factor authentication (MFA) for login.
  - Complex login passwords are used.
  - Employees use a VPN solution to log in remotely when required.

- **Network Security:**
  - The organization has Palo Alto Next Gen firewalls.
  - The firewalls have been configured by the network.
  - The firewalls get audited every year by the network team.
  - The firewalls get regular updates.
  - The IT team has up-to-date network diagrams. The diagrams include the various cloud environments.
  - The network is segmented using VLANs.

- **Physical Security:**
  - Oscorp is a highly secure facility, with state-of-the-art CCTV cameras everywhere.
  - Oscorp takes physical security very seriously.
  - They do extensive vetting for all their employees.
  - They have 24/7 monitoring for their research labs and physical facilities.

- **Data Security:**
  - Oscorp does not have a DLP solution.
  - All data resides in Microsoft Azure cloud and Microsoft Office 365.
  - Key critical application is a SaaS service from Horizon Labs.

- **Policy:**
  - There is one generic IT policy in place.

- No formal information security policy exists.
- There are no data governance policies or information classification.

- **Cyber Security Detection and Response:**
  - There is no detection or response capabilities.
  - The IT team responds to alerts from the anti-virus (Microsoft Defender).
  - No SIEM is in place.

- **Security Education and Awareness:**
  - All employees are required to onboard using an induction web training module. The module includes basic instructions about cyber security.