Current Oscorp cyber security team:

- Cyber security analyst: generalist, responds to cyber incidents as they come. Reports to Oscorp's IT manager.

- Network engineer: manages the firewalls. Reports to the Network Team Leader.

- Cyber Security Consultant: your new role it Oscorp. You will initially report to the IT manager.

Oscorp Current Cyber Security Controls:

- Organisational governance:
  - CEO has a clear business strategy for the business. However, roles and responsibilities for cyber security haven't been defined. They're assigned to the IT team. There is no 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 get tested periodically

- Vulnerability management:
  - Oscorp have purchased Qualys vulnerability scanner.
  - The IT team uses Qualys on an ad-hoc basis.
  - There is no formal vulnerability management program in place.
  - Large number of high and severe vulnerabilities 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:

    - Oscorp doesn’t perform any third-party risk management.
    - Contracts are reviewed by procurement and finance, not IT.

- Identity and Access Management:
    - 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 organisation does not use two-factor authentication for login
    - Complex login passwords are used
    - Employees use a VPN solution to login remotely when required

- Network security:
    - The organisation 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 have up to date network diagrams. The diagrams include the cloud the environment.
    - 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 very seriously
    - They do extensive vetting for all their employees
    - The have a 24/7 monitoring for their research labs and physical facilities

- Data Security:
    - Oscorp doesn’t 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
    - There is no data governance policies or information classification

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

- Security Education and Awareness:

- All employees are required to do an induction web training module. The module includes basic instructions about cyber security.