Branden Barnes

CS 465

11/10/2024

Organizational Structure, Planning and Deployment, and Human Factors

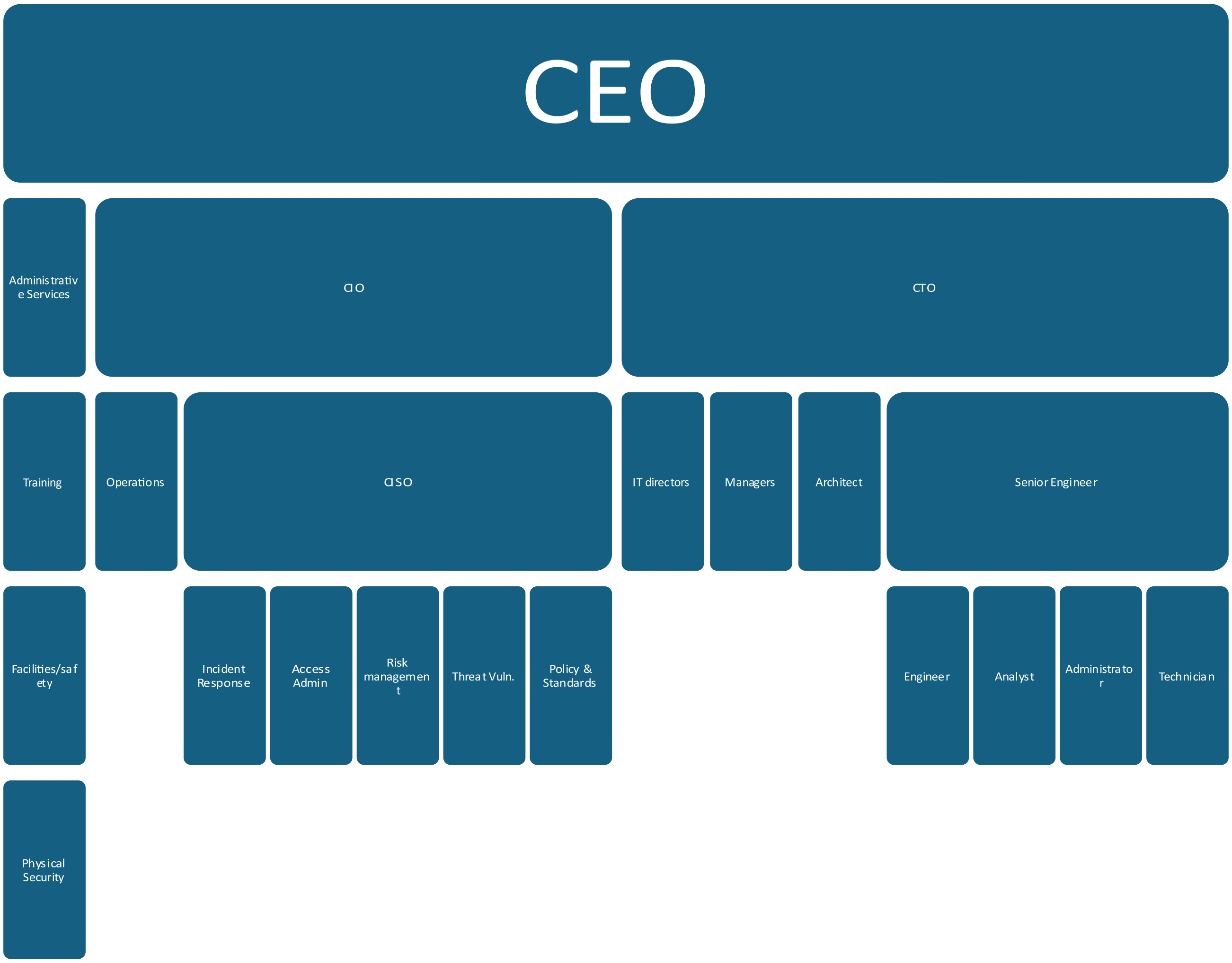
In the context of ABC Inc., which is a large on-line electronic product company, answer the following questions.

1. **State three regulations and standards that it should comply with.**
2. **List the responsibilities (roles) of the Information Security Officer of ABC Inc.**
3. **Suggest a reporting structure (as a diagram) for ABC Inc., assuming that it has 2 million customers, 2000 employees, approximately 20000 transactions each day, and $2 billion sales. Give a brief justification.**
4. **Describe an incident response plan for ABC Inc. Write it as a list of steps with a brief description for each**

1. Common Vulnerabilities and Exposures, Payment Card Industry Data Security Standard, 5 U.S. Code 552a – Records maintained on individuals (Privacy Act 1974).

2. Responsibilities of the ISO include: Implementing security policies and procedures, Regulatory compliance, Disaster recovery, Incident response and management, leading a team of security professionals, risk management/assessment, cybersecurity, monitor compliance, information security strategy, etc. In the context of ABC inc., The CISO will create and implement a program and plan for information security across the company. He will do this by updating regulations and standards and oversee the information security team in their efforts to make the company safe.

3.



Hierarchy is important for reporting structure. Since ABC inc., is a larger company a centralized specialization structure Is necessary. I broke the structure up into three many officers who report to the CEO. Those officers are the administrative services, Chief Information officer, and Chief Technology officer. Under them is their respected middle management then lower management.

The more departments allow for specialization and organization.

4. An incident response plan starts with planning. Planning must ensure that appropriate staff are available to respond to incidents. Next step is detection. Incident detection will determine whether an

incident can potentially become a threat or attack. Next is reaction. Incident reaction refers to mitigating an incidents escalation and containment. Last is recovery. Incident recovery focuses on damage assessment, forensics, evidence; and evaluation, identification, and monitoring of the vulnerabilities exposed in the attack.