MEP - Assignment I

Shivcharan. T
205001100
CSE-B

(1)
- When it comes to self-interest, it refers to the pursuit of one's own personal advantage or well-being.
- It is the idea that individuals actions & decisions are primarily instructed to maximize their own benefit.
- Taking the customs & religion into account, self interest can be influenced & shape the ethical values of a person.
- Cultural Customs:
  - Customs often contribute to social harmony, giving a sense of identity & belonging in a community.
  - Following these customs can be viewed as an ethical choice which promotes collective well being of the society.
- Morality in Religion:
  - Religious teaching provide moral guidelines shaping ethical behaviours.
  - Believing these principles will give a greater purpose & fulfillment to one's own self interest
  - Eg: Say a person not consuming forbidden food or drinks such as alcohol, will make them ethically moral & increase satisfaction.
- Ethical Egoism:
  - This argues for actions that prioritize self interest
  - This perspective suggests that acting in one's own best interest is not only ethically acceptable but also fundamental aspect of ethical decision making.
- Conflict of interest:
  - Conflict may arise when cultural customs or religious clash with one's self interest.
  - Resolving these conflicts requires individuals to consider the impact of their actions on both personal & community level.

In conclusion, customs & religion play a major role in influencing one's self interest & decision making. Accustoming such disciplines leads to a moral & ethical ways of self-interest.

(2) Advanced Cyber Threats are highly sophisticated forms of cyber attacks that

leverage advanced technologies & strategies to compromise digital data & systems. Few of the threats are:

i) Ransomware Attacks:

- Ransomware involves the encryption of a victims file system with an attacker demanding a ransom.
- They pose a risk to organization, disrupting work & compromising sensitive data.

ii) Nation-State Espionage:

- Threat in this are actors engaging in political, economical & military purposes.
- These actors use advanced technology to infiltrate networks of government or corporation seeking significant geopolitical implications.

iii) Cloud-based Threats:

- As an organization, many rely on cloud services to operate their services online.
- They store vast amounts of sensitive data, breaches include data loss, denial of service & unauthorized access.

iv) IoT based Threats:

- The IoT devices are vulnerable & insecure & attackers can exploit them. Compromised IoT devices can be used for DDoS attacks & disruption of IoT devices

v) Supply chain Attack:

- These involves compromising the security of product or service during their development or distribution. Attackers target the software updates, hardware components or other third party services to infiltrate the target.

(3) Asserting ownership in cybersecurity involves establishing control, accountability & responsibility over digital assets. Various such methods are:

i) Access control:

- By ensuring that only authorized users have access to specific resources thereby asserting control & ownership over digital assets.

ii) Encryptions:

- Encryption safeguards data's confidentiality & integrity, allowing to protect sensitive information which they own.

iii) Digital Signatures & certificates:

- These provide a mean to confirm the identity & integrity of a person enabling to communicate & allow users to digital assets.

iv) Authentication:

- Methods such as biometrics, multifactor authentication & strong password policies are crucial for verifying the identity.

v) Network Segmentation:

- This allows organization to control over different parts of their infrastructure instead of having as a whole keeping the assets isolated.