Management and Ethical Practices - Assignment

Saboorivasan. V
205001085
CSE-B

(1) Customs and Ethics

⇒ Customs often form the basis of cultural norm and values. Cultural relativism suggests that ethical standards are relative to cultural practices.

⇒ Customs can contribute to formation of social contracts with a community. These contracts establish expectations for ethical behaviour and cooperation for mutual benefit.

Religion and Ethics

⇒ Acting in accordance with religious teachings is seen as not only a moral duty but also in one's self-interest to secure a favourable position.

⇒ Religions often provide comprehensive set of moral guidelines that dictate proper conduct, adhering to these guidelines is considered virtuous and lead to positive consequences.

Intersection of Customs, Religion and Self-Interest

⇒ Customs and religion can provide individuals with ethical frameworks that guide their behaviour.

⇒ Adhering to ethical practices within cultural or religious contexts can bring social and personal benefits. These may include community acceptance, positive relationships and a sense of purpose to an individual's self-interest.

⇒ Conflicts may arise when customs or religious principles clash with personal self-interest. In conclusion the interplay between customs, religion and self-interest in ethics is dynamic and varies across cultures and individuals.

---

(2) ## Future of Risk in Digital Era

⇒ The future of risk in digital era is becoming increasingly complex and challenging due to rise of advanced cyber threads.

⇒ Malacious software continues to evolve with new features and evasion techniques. Ransomware attacks in particular have become more targeted and destructive.

⇒ Cybercriminals are constantly searching for and exploiting vulnerabilities in software or hardware before developers can create patches.

⇒ As organizations move their data and operations to the cloud, new security challenges arise. Insecure interfaces and unauthorized access to cloud resources can result in large scale data breaches.

⇒ Critical infrastructure like power grids, transportation systems and healthcare facilities is a prime target for nations and states.

⇒ AI and ML are being used by cyber attackers to enhance speed and effectiveness of their attacks. This includes automating tasks such as reconnaissance, target selection and evasion of security measures.

⇒ Addressing advanced cyber threats requires global collaboration. Nations, organizations and experts must work together to share threat intelligence, establish norms for responsible behaviour in cyberspace.

In conclusion, the future of risk in digital era is closely tied to the evolution of advanced cyber threats. To mitigate these risks, individuals and governments must invest in robust cybersecurity measures.

---

(3) Asserting Ownership in Cyber Security

⇒ Asserting ownership in cybersecurity is crucial for protective digital assets, ensuring data privacy and maintaining integrity of systems.

⇒ Implementing strong authentication mechanisms, including multi-factor authentication ensures that only authorized users have access to sensitive systems and data. Defining and enforcing access policies that dictate who can access what resources under specific conditions.

⇒ Using data signatures for code and software ensures only authenticated and approved code is executed. This prevents intro of malicious code into systems.

⇒ Defining policies that online acceptable and unacceptable behaviour on organizational networks and systems establishing ownership.

⇒ Implementing robust logging and monitoring solutions enables the tracking of user activities and system events.

⇒ Clearly defining data ownership in legal agreements, including terms of use and data sharing agreements, helps establish legal frameworks for asserting ownership and protecting digital assets.

⇒ Educating employees about cybersecurity best practices and their responsibilities regarding digital assets helps in creating security aware culture where individuals understand and respect ownership boundaries.

In summary, asserting ownership in cybersecurity involves multi faceted approach that includes technical controls, policy enforcement and strong focus on user awareness and education.