COMPUTER SECURITY STRATEGY Module 1

COMPUTER SECURITY STRATEGY

SUMMERY

Matched Branch:	0
Partially Matched Branch:	9
Mismatched Branch:	7
Extra Branch:	2
Total Match:	23.53 %
Concept Match:	31.25 %
Link. Phr. Match:	10.53 %
Misconception:	100.0 %
Hierarchy Match:	11.19 %

Grade: 11.57%

aspects of security strategy

- Implementation and Mechanisms
  - illustrated by
    - Method used by the security scheme
  - portrayed by
    - Security Implementation
      - involves these four complementary courses of action
        - Prevention
          - for example
            - Secure Encryption Algorithms
              - with the result of
                - Prevent unauthorized access to encryption keys
        - Response
          - with the purpose of
            - Upon detection, being able to halt an attack and prevent further damage
        - Detection
          - for instance
            - Intrusion Detection Systems (IDS)
              - with the purpose of
                - Detection of denial of service (DoS) attacks
        - Recovery
          - for instance
            - Use of backup systems
- Correctness and Assurance
  - characterized by
    - Viability of security scheme
      - encompasses
        - Both the system design and system implementation
  - composed of
    - Assurance
      - defined by
        - Degree of confidence one has that the security measures work as intended to protect the system and the information it processes
    - Evaluation
      - involves
        - Testing and formal analytic or mathematical techniques
      - described by
        - Process of examining a computer system with respect to certain criteria
- Specification and Policy
  - represented by
    - Purpose of the security scheme
  - elaborated by
    - Security Policy
      - depicted by
        - Formal statement of rules and practices that specify or regulate how a system or organization provides security services to protect sensitive and critical system resources
          - considering these trade-offs
            - Ease or use versus security
            - Cost of security versus cost of failure and recovery
          - deliberating these factors
            - Potential threats and the likelihood of attacks
            - Value of the assets being protected
            - Vulnerabilities of the system