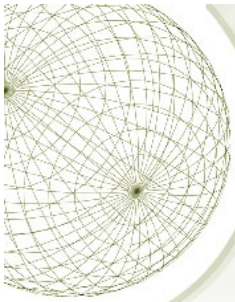
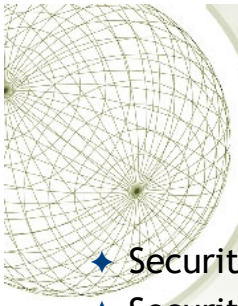


Curtin University

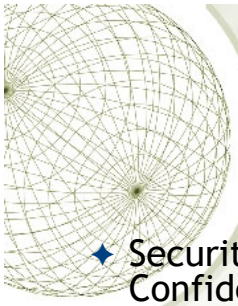
Fundamental Concepts of Data Security

Revision



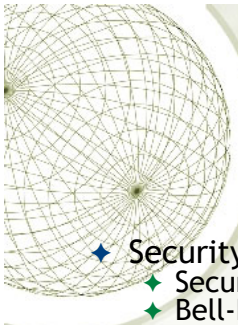
Major Topics

- Security systems (AIC)
- Security controls
- Risk assessment and change management
- Business impact analysis, disaster recovery planning, and testing, incident response
- Data backup, data masking and data erasure
- Ethics



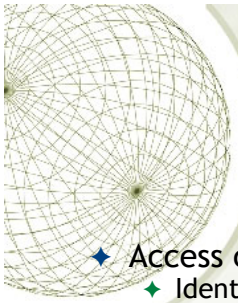
Security Systems

- Security triad: Availability, Integrity, Confidentiality
- Security management responsibilities
- Security requirements
  - Availability
  - Integrity
  - Confidentiality
- Addressing general security goals
  - Availability
  - Integrity
  - Confidentiality



Security Systems

- Security models
  - Security policy vs security models
  - Bell-Lapadula (confidentiality): no write down, no read up, read+write same level
  - Biba (integrity): no write up, no read down, service request
  - Clark Wilson (integrity): authorized/unauthorized users + data consistency
- Virtualization and cloud computing
  - Virtualization: pros and cons
  - Cloud computing types: public, private, community, hybrid
  - Cloud computing services: PaaS, IaaS, SaaS
  - Cloud computing issues

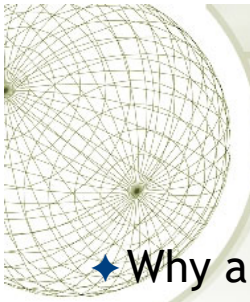


Security Controls

- Access control concepts
  - Identity, Authentication, Authorization, Accountability, Password management
- Controls
  - By nature: Technical, Physical, Administrative
  - By functionality: Deterrent, Preventive, Detective, Corrective, Recovery
- Commonly used security methods
  - Least privilege, Defense-in-depth, Minimization, Keep things simple
  - Compartmentalization, Use choke points, Fail securely/safely
  - Leverage unpredictability, Separation of duties

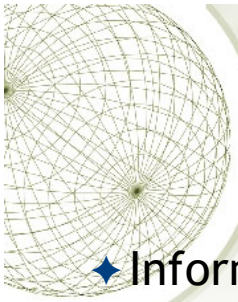
Data Backup

- Infrastructure: local, server, enterprise, SAN
- Types: full, incremental, differential
- What to backup
- Backup rotation
- Issues



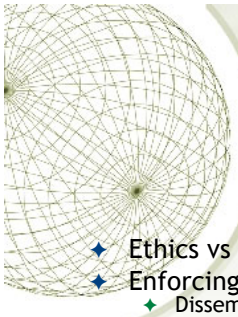
Data Masking

- Why and when
- Requirements
- Methods: substitution, shuffling, variance, nulling out, encryption, masking out
- Types: static, dynamic
- Pros and cons of each type
- Cloud data masking



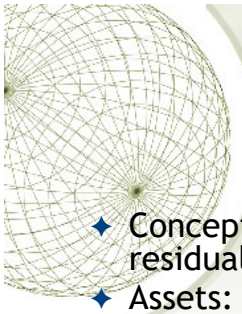
Secure Data Erasure

- Information classification
- Media types
- Validation
- Categories: disposal, clearing, purging, destroy



Ethics

- Ethics vs laws
- Enforcing policy
  - Dissemination, review, comprehension, compliance, enforcement
- Professional organisations and their role in promoting ethical behaviour
- Causes of unethical behaviour
  - Ignorance, Accident, Intent
- Preventing unethical behaviour
  - Education & training, penalty, prosecution
- Ethical issues
  - IP & software infringement
  - Security rights, Hackers
  - Illegal downloading/sharing of materials
  - Privacy issue: private vs public information, corporate handling of personal data
  - Misuse of corporate resources



Risk Management

- Concepts: vulnerability, threat, likelihood, risk, total risk, residual risk
- Assets: tangible vs intangible
  - Asset value, SLE, EF, ARO, ALE
  - Risk matrix
- Risk analysis's goals
- Risks analysis approaches: quantitative vs qualitative
  - Pros and cons
- Strategies to address risk
  - Defend, Mitigate, Transfer, Terminate, Accept
- Change management
  - Goals/objectives
  - Procedures

Business Continuity Planning

- Business impact analysis
  - Critical activities, resources, and impacts
  - Important parameters: RPO, RTO, MTD
- Disaster recovery planning
  - Offsite facility: hot, warm, cold
  - Procedures
  - Roles and responsibilities
  - Contacts: internal & external
- Testing BCP
  - Methods
  - Frequency and timing
- Review and Update

Incident Response Planning

- Incidents vs disasters
- Phases: detection/triage, containment, investigation, analysis, tracking, recovery
- Preparation: IR team, organisational preparation, response kit, documentation
- IR procedures
- Post-incident activity