Cybersecurity Fundamentals

Course assessment

- Test – 30% (Final ass) = 12/30
- Group Assignment – 30% (4 persons)
  - Case study – Risk and threat assessment – 15%
  - Case study – Countermeasures – 15%
- Quiz – 40%
  - 5 quiz (Tutorial class)
  - 8%

MCQ for Quiz and Test.

70%
CW 28/70

Lecture 1

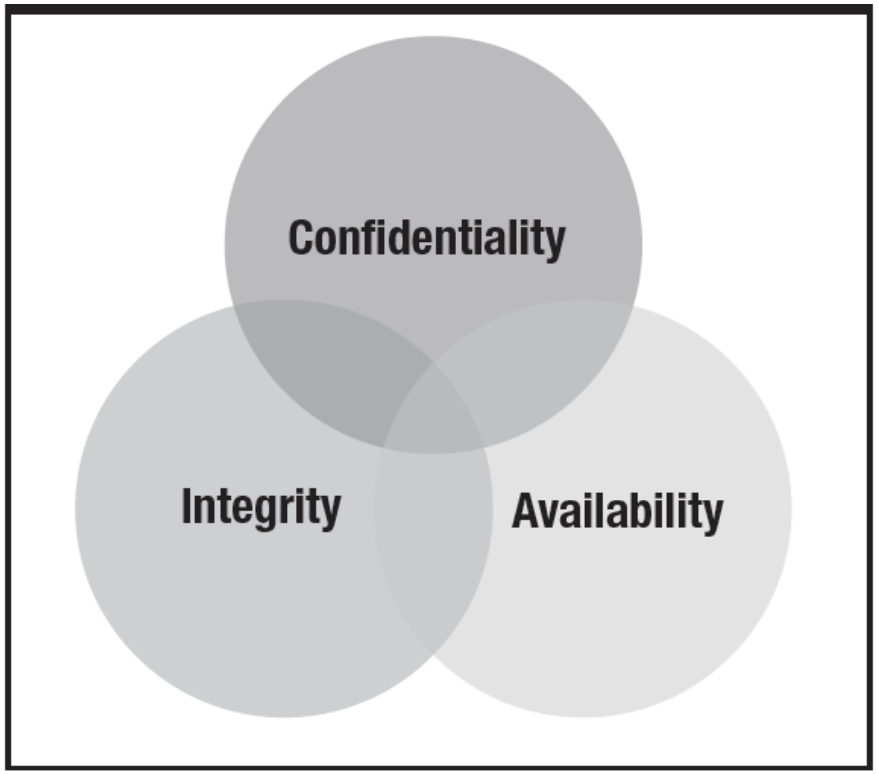
Introduction to Cybersecurity

Introduction to Cybersecurity

- Computer security - Network security - Information security - Cybersecurity.
- All of these terms are used to describe the protection of information assets.
- Why have there been so many changes in the way we refer to security?
- Safeguarding information has been a priority for as long as people have needed to keep information secure and private.
- But as time and technology move forward, so do the demands of security.
- The objective of information security is threefold, involving the critical components of confidentiality, integrity and availability.

Introduction to Cybersecurity

- All three components are concerned with the protection of information.
- Confidentiality means protection from unauthorized access.
- Integrity means protection from unauthorized modification 修改
- Availability means protection from disruptions in access. 中斷



Introduction to Cybersecurity

- New trends in mobility and connectivity present a broader range of challenges than ever before as new attacks continue to develop along with emerging technologies.
- Cybersecurity professionals must be informed and flexible to identify and manage potential new threats, such as advanced persistent threats (APTs), effectively.
- APTs are attacks by an adversary who possesses sophisticated levels of expertise and significant resources, which allow the attacker to create opportunities to achieve its objectives using multiple attack vectors.
- In order to successfully protect their systems and information, cybersecurity professionals must demonstrate a high degree of situational awareness.

Situational awareness

- This type of awareness takes time to cultivate, because it usually develops through experience within a specific organization.
- Each organization has its own distinct culture. Therefore, it is critical for cybersecurity professionals to have an awareness of the environment in which they operate.
- Central to this awareness is an understanding of key business and technology factors that affect information security.
- Numerous factors, both internal and external, can directly impact an organization and its security needs, including:
  - Business plans and business environment
  - Available information technology, security process or systems in particular

Situational awareness

- Both of these factors tend to be situational in nature.
- Business environment in particular tends to drive risk decisions. For example, a small start-up company may be much more tolerant of risk than a large, well-established corporation.
- With respect to technology, there are many factors that can impact security, such as:
  - Platforms and tools used
  - Network connectivity (internal, third-party, public)
  - Level of IT complexity
  - Operational support for security
  - User community and capabilities
  - New or emerging security tools

Situational awareness

- When evaluating business plans and the general business environment, consider drivers, such as:
  - Nature of business
  - Risk tolerance
  - Security profile
  - Industry trends for security
  - Mergers, acquisitions and partnerships
    - Consider type, frequency and resulting level of integration
  - Outsourcing services or providers
- Although business and technology drivers cannot all be predicted with certainty, they should be anticipated reasonably and handled as efficiently as possible.

Cybersecurity skills gap

- Cybersecurity is a field that demands skilled professionals who possess the foundational knowledge, education and thought leadership necessary to confront the difficulties that accompany constant technological change.
- Advanced threat vectors, emerging technologies and myriad regulations require cybersecurity professionals to be skilled in technology as well as business and communications.
- Cybersecurity addresses both internal and external threats to an organization's digital information assets by focusing on critical electronic data processes, signal processing, risk analytics and information system security engineering.

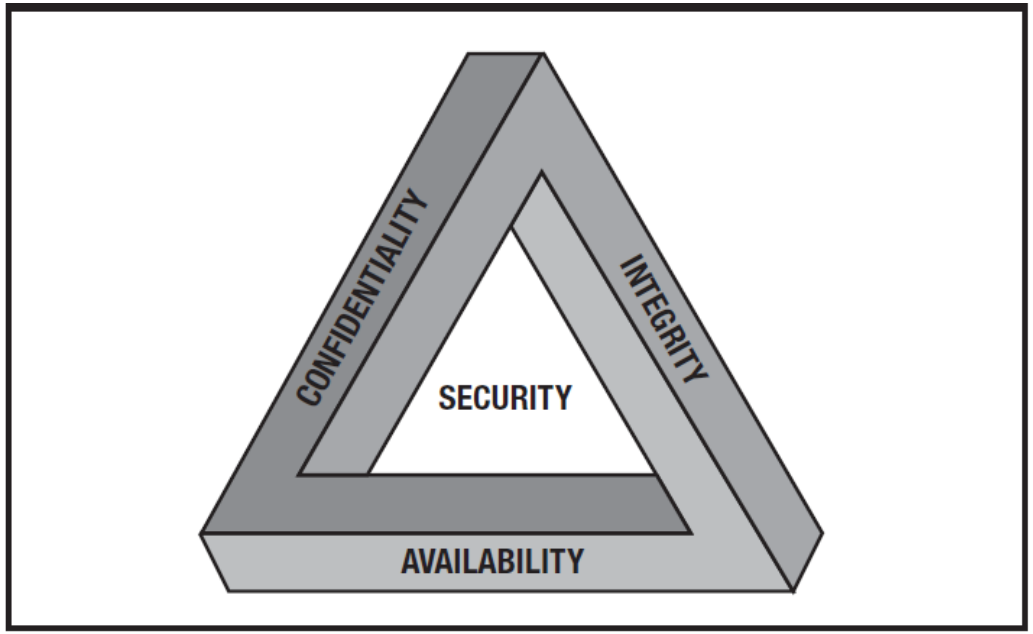
Cybersecurity objectives

- In their cybersecurity frameworks, both the National Institute of Standards and Technology (NIST) and the European Union Agency for Network and Information Security (ENISA) have identified five key functions necessary for the protection of digital asset:
  - Identify: Use organizational understanding to minimize risk to systems, assets, data and capabilities.
  - Protect: Design safeguards to limit the impact of potential events on critical services and infrastructure.
  - Detect: Implement activities to identify the occurrence of a cybersecurity event.
  - Respond: Take appropriate action after learning of a security event.
  - Recover: Plan for resilience and the timely repair of compromised capabilities and services.

復原能力

Cybersecurity objectives

- To better understand cybersecurity and the protection of cyber assets, it is helpful to consider three key concepts that are used to guide security policies:
  - Confidentiality
  - Integrity
  - Availability



Cybersecurity objectives

信息披露

- Confidentiality is the protection of information from unauthorized access or disclosure.
  - Different types of information require different levels of confidentiality, and the need for confidentiality can change over time.
- Integrity is the protection of information from unauthorized modification.
  - For example, if a bank transfers US $10,000 to another financial institution, it is important that the amount does not change to US $100,000 during the exchange.
  - The concept of integrity also applies to software and configurations.
- Availability ensures the timely and reliable access to and use of information and systems.
  - This would include safeguards to make sure data are not accidentally or maliciously deleted.
  - This is particularly important with a mission-critical system, because any interruptions in its availability can result in a loss of productivity and revenue.

Cybersecurity objectives

- The impacts, potential consequences and methods of control of confidentiality, integrity and availability are:

Requirement	Impact and Potential Consequences	Methods of Control
Confidentiality: the protection of information from unauthorized disclosure	Loss of confidentiality can result in the following consequences: • Disclosure of information protected by privacy laws • Loss of public confidence • Loss of competitive advantage • Legal action against the enterprise • Interference with national security	Confidentiality can be preserved using the following methods: • Access Controls • File Permissions • Encryption
Integrity: the accuracy and completeness of information in accordance with business values and expectations	Loss of integrity can result in the following consequences: • Inaccuracy • Erroneous decisions • Fraud	Integrity can be preserved using the following methods: • Access controls • Logging • Digital Signatures • Hashes • Encryptions
Availability: the ability to access information and resources required by the business process following consequences:	Loss of availability can result in the following consequences: • Loss of functionality and operational effectiveness • Loss of productive time • Interference with enterprise's Objectives	Availability can be preserved using the following methods: • Redundancy • Backups • Access Controls

Contextualizing Cybersecurity

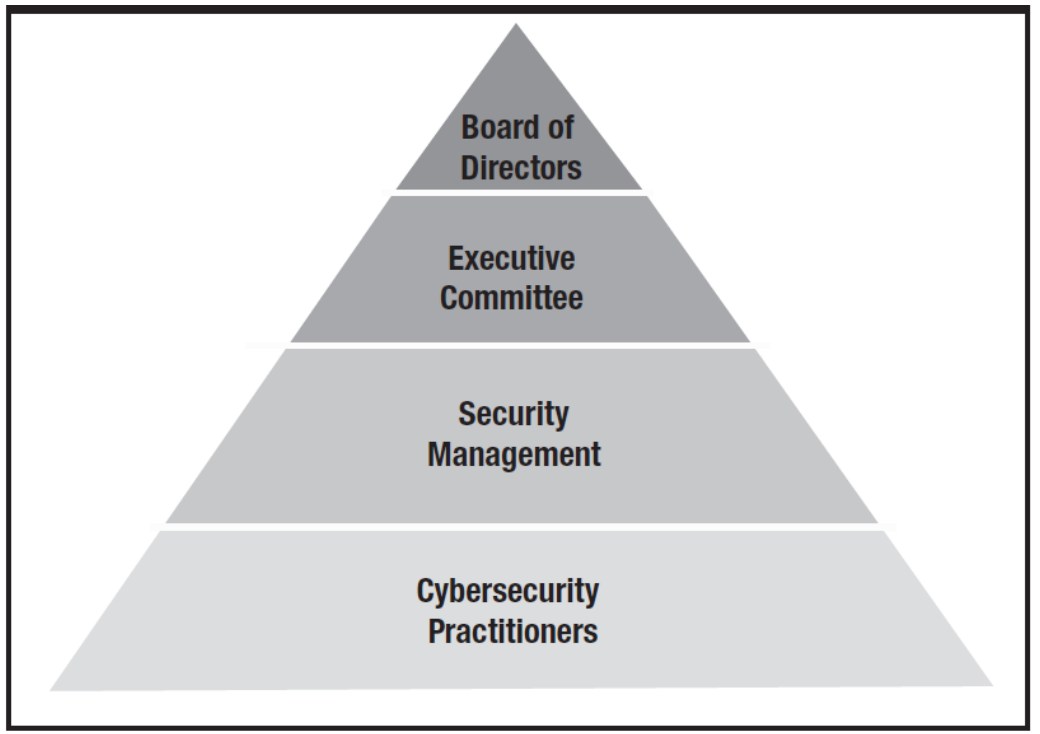
- Governance, Risk Management and Compliance
  - All organizations have a responsibility and duty to protect their assets and operations, including their IT infrastructure and information.
  - This is generally referred to as governance, risk management and compliance (GRC).
  - Governance is the responsibility of the board of directors and senior management of the organization.
  - A governance program has several goals:
    - Provide strategic direction
    - Ensure that objectives are achieved
    - Ascertain whether risk is being managed appropriately
    - Verify that the organization's resources are being used responsibly

Contextualizing Cybersecurity

- Risk management is the process by which an organization manages risk to acceptable levels.
  - Risk management requires the development and implementation of internal controls to manage and mitigate risk throughout the organization, including financial and investment risk, physical risk and cyber risk.
- Compliance is the act of adhering to, and the ability to demonstrate adherence to, mandated requirements defined by laws and regulations.
  - It also includes voluntary requirements resulting from contractual obligations and internal policies.

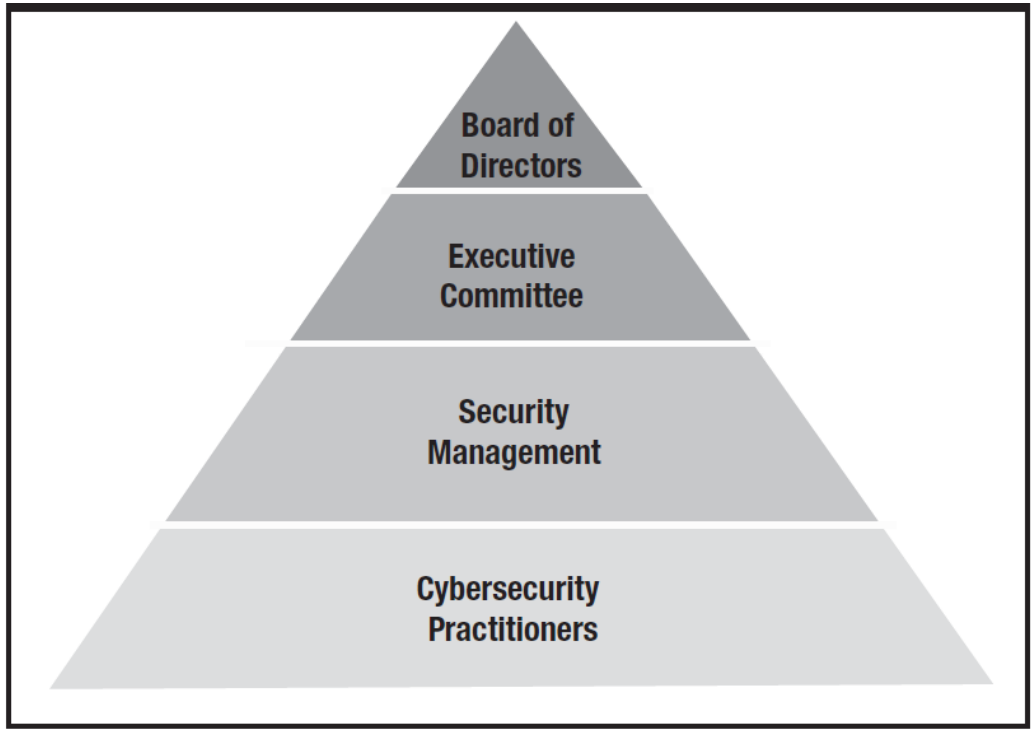
Contextualizing Cybersecurity - Roles

- Board of Directors
  - Cybersecurity governance requires strategic direction and impetus. 推动力
  - Effective governance can be accomplished only by senior management involvement in approving policy and by appropriate monitoring and metrics coupled with reporting and trend analysis.
  - The board should periodically be provided with the high-level results of comprehensive risk assessments and business impact analyses (BIAs).
  - Board members to identify the key assets they want protected and verifying that protection levels and priorities are appropriate to a standard of due care.



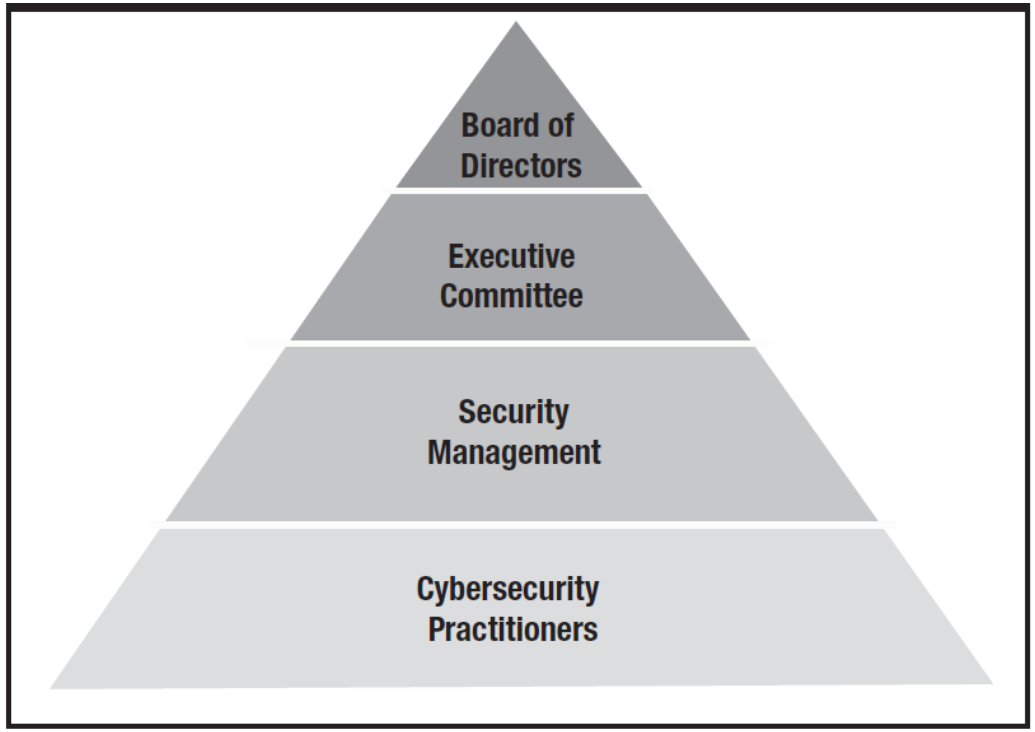
Contextualizing Cybersecurity - Roles

- Executive Management
  - An organization's executive management team is responsible for ensuring that needed organizational functions, resources, and supporting infrastructure are available and properly utilized to fulfill the directives of the board, regulatory compliance and other demands.
  - Generally, executive management looks to the chief information security officer (CISO) or other senior cybersecurity manager to define the information security program and its subsequent management.
  - The Cybersecurity manager is also expected to provide education and guidance to the executive management team.



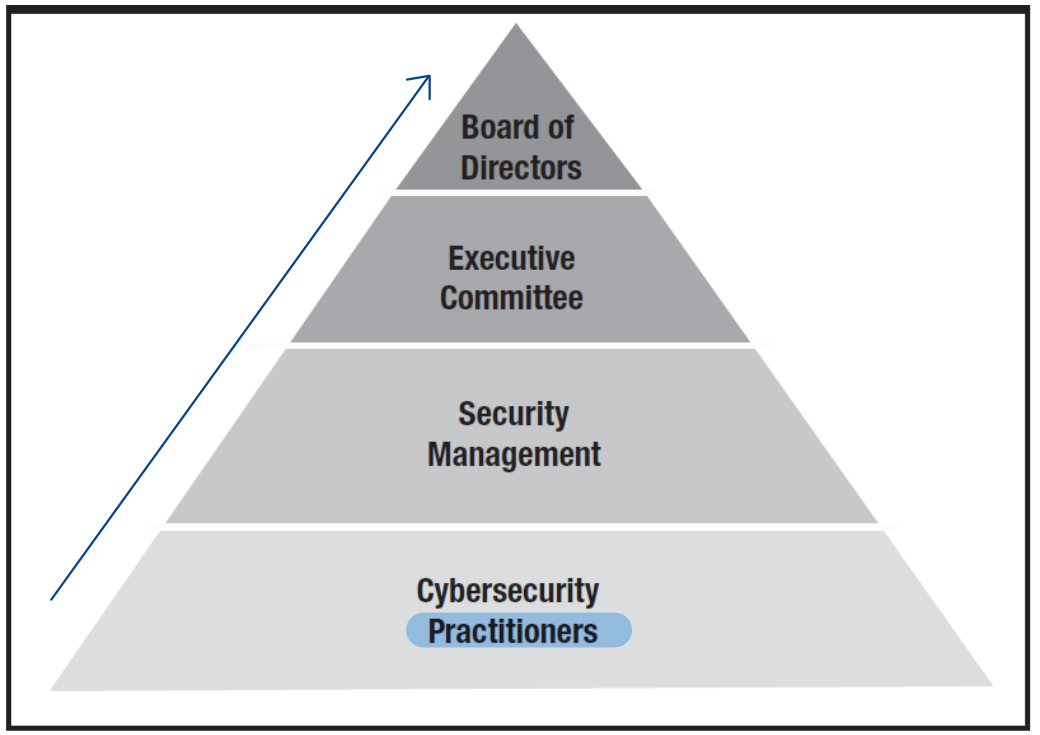
Contextualizing Cybersecurity - Roles

- Security Management
  - The chief information security officer (CISO) or chief security officer (CSO) oversees information security and cybersecurity.
  - Generally, the cybersecurity manager will be responsible for:
    - Developing the security strategy
    - Overseeing the security program and initiatives
    - Coordinating with business process owners for ongoing alignment
    - Ensuring that risk and business impact assessments are conducted
    - Developing risk mitigation strategies
    - Enforcing policy and regulatory compliance
    - Monitoring the utilization and effectiveness of security resources
    - Developing and implementing monitoring and metrics
    - Directing and monitoring security activities
    - Managing cybersecurity incidents and their remediation, as well as incorporating lessons learned



Contextualizing Cybersecurity - Roles

- Practitioners
  - In most organizations, cybersecurity is managed by a team of subject matter experts and cybersecurity practitioners, including security architects, administrators, digital forensics and network security specialists.
  - Together they design, implement and manage processes and technical controls and respond to events and incidents.



Contextualizing Cybersecurity - Domains

- Cybersecurity Concepts
  - Basic risk management
  - Common attack vectors and threat agents
  - Patterns and types of attacks
  - Types of security policies and procedures
  - Cybersecurity control processes
- Security Architecture Principles
  - Common security architectures and frameworks
  - System topology and perimeter concepts
  - Firewalls and encryption
  - Isolation and segmentation
  - Methods for monitoring, detection and logging

Contextualizing Cybersecurity - Domains

- Security of Networks, Systems, Applications and Data
  - Process controls
    - Risk assessments
    - Vulnerability management
    - Penetration testing
  - Best practices for securing networks, systems, applications and data
    - System and application security threats and vulnerabilities
    - Effective controls for managing vulnerabilities
- Incident Response
  - Incident categories
  - Disaster recovery and business continuity plans
  - Steps of incident response
  - Forensics and preservation of evidence

Contextualizing Cybersecurity - Domains

- Security Implications and Adoption of Evolving Technology
  - Mobile devices
  - Cloud computing and storage
  - Digital collaboration
  - Blockchain
  - IOT devices

Domain 1.

1) Information Security
- Security that focuses on all of our information.
This includes paper documents, voice information, data knowledge.

2) IT security
- Security that focuses on the hardware and software.
- This includes Computers, servers, network, hardware, software, and data being communicated.

3) Cybersecurity
- Everything from IT security that is accessible on the web

4) Confidentiality 機密
- The act of holding information in confidence, not to be released to unauthorized individuals.

5) Integrity
- How we protect modifications of the data and the systems to ensure data has not been altered. 更改

6) Availability
- Ensure authorized people can access the data they need when they need it.

7) Applications for confidentiality.
- Encryption for Data at rest, full disk encryption.
- Secure transport encryption protocols for data-in-motion (SSL, TLS or IPSEC)

8) Best pratices for data-in-use
- Clean desk
- No shoulder surfin
- Screen view angle protector
- PC Locking

9) Other factors of confidentiality
- Strong passwords
- MFA (Multi-Factor Authentication) - ID, password, finger print
- Masking
- Access control
- Need-to-know
- Least Privilege

10) Threats to confidentiality
- Attacks on encryption (cryptoanalysis)
- Social engineering
- Key loggers
- Cameras
- Steganography 隱密傳輸
- IOT devices.

11) Applications for Integrity
- Cryptography
- Check Sums
- Message Digests
- Digital Signatures
- Non Repudiation
- Access control

12) Threats to Integrity
- Alternations of data
- Code injections.
- Cryptoanalysis.

13) Applications for Availability
- IPS / IDS
- Patch management.
- Redurancy on hardware power.
- Disks (RAID)
- Traffic Paths
- Service Level Agreement (SLA)

14) Threats to Availability
- Malicious attack (DDoS, physical, system, compromise, staff)
- Application failures.
- Component failure.

15) The DAD Triad 三合一
- Disclosure 披露
- Alteration 改動
- Destruction 毀壞

16) Disclosure

- Someone not authorized to access certain information

17) Alteration

- Data has been changed.

18) Destruction

- Data or systems have been destroyed or have become inaccessible.

19) IAAA

- Identification
- Authentication
- Authorization
- Accountability

20) Indentification

- Using a piece of information to identify who you are
- Examples include name, username, ID, number, employee number, SSN.

21) Authentication

- Proving that a user is genuine, and not an imposter.

22) Type 1 of Authentication.

- A type of authentication that requires the user to provide something that they know, such as a password or PIN.
- This is the weakest form of authentication.

23) Key Stretching

- A technique used to increase the strength of stored passwords. It adds additional bits (called salts) and can help thwart brute force and rainbow table attacks.

24) Brute force attack

- The password cracker tries every possible combination of characters.

25) Clipping levels

Put in place to prevent administrative overhead

- Allows authorized users who forget or mistype their password to still have a couple of extra tries.
- Prevents password guessing by locking the user account for a certain timeframe.

26) DOD password History.

- Set to remember 24 password.

27) DOD password age

- 90 days

28) DOD min password age

- 2 days

29) DOD min password length

- 8 characters

30) Type 2 Authentication

- A type of authentication that requires the user to provide something that they have, such as a key fob, electronic chip, or smart card.

31) Single-use password

- Similar to one time pads where passwords are only valid once.
- This is a Type 2 authentication.

32) Smart cards and Tokens

- Cards that contain a computer circuit using an ICC (Integrated Circuit chip)

33) Contact Cards

- Cards that are inserted into machines to be read

34) Contactless cards

- Cards that don't require insertion for payment.

35) Magnetic Stripe cards

- A type of card that stores a limited amount of data by modifying the magnetism of tiny iron-based particles contained in a band on the card.

36) Tokens

- Small electronic devices that change user passwords automatically.

37) HMAC - based onetime password (HOTP)

- Shared secret and incremental counter, generate code when asked, valid till use.

38) Time - based one-time password (TOTP)

- A one-time password that changes after a set period of time.

39) Type 3 Authentication

- A type of authentication that requires the user to provide something that they are, such as fingerprint, handprint, retinal pattern, face, or voice.

40) False Rejection Rate (FRR)

- A measurement of valid users that will be falsely rejected by the system. This called a type 1 error.

41) False Acceptence Rate (FAR)

- A measurement of the percentage of invalid users that will be falsely accepted by the system. This called Type II error.

* Type II errors are MORE DANGEROUS than Type I error

42) Physiological Characteristic

- Uses the shape of the body, these do not change unless a drastic event occurs.

43) Behavioural Characteristic

- Uses the pattern of behaviour of a person, these can change, but most often revert back to the baseline.

44)