IT2775 Operations Security

Introduction

KH Yee
Simon_yee@nyp.edu.sg
6550-1802

NANYANG POLYTECHNIC

Objectives

- What is Operations Security?
  - What are enterprise networks?
- Need for Operations Security
- Operations Security Process
- Key Areas of Operations Security

Topics Covered:

- Introduction
- BCP – Business Continuity Planning
- Malware Defence and Management
- Backup and Recovery
- Backup Planning
- User Account Management
- Patch Management
- Configuration Management
- Security Configuration Management
- Personnel Management
- MSSP – Managed Security Services Provider
- ISCM – InfoSecurity Continuous Monitoring

Assessment Schedule

- Please refer to Blackboard for this

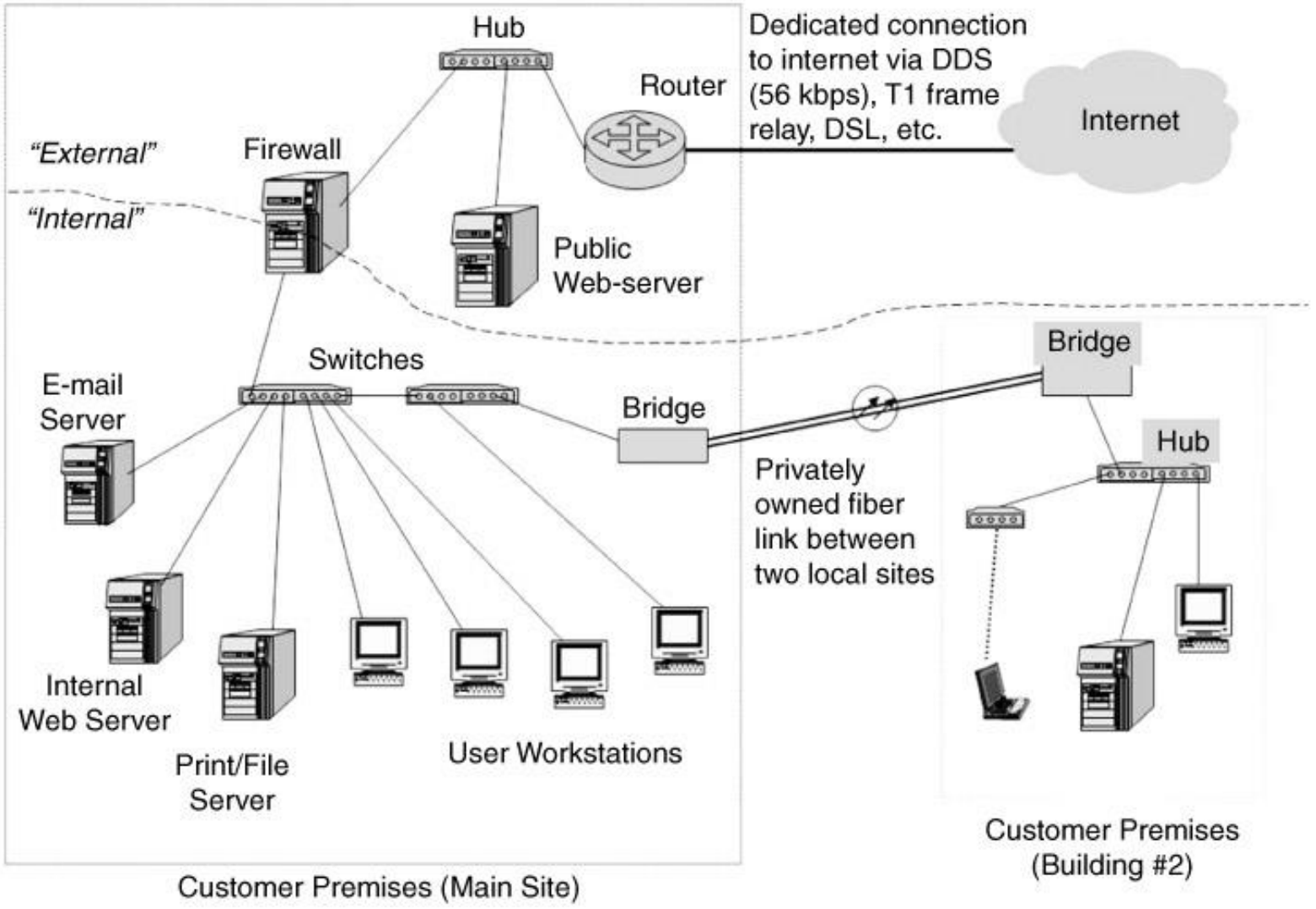
What is Operations Security?

- Operations Security:
  - Protection and control of info processing assets in both centralized and distributed environments.
  - Daily tasks required to keep services operating reliably and efficiently.
  - With respect to an enterprise IT network.
- Not to be confused with Operations Security (OPSEC) as defined by the military.

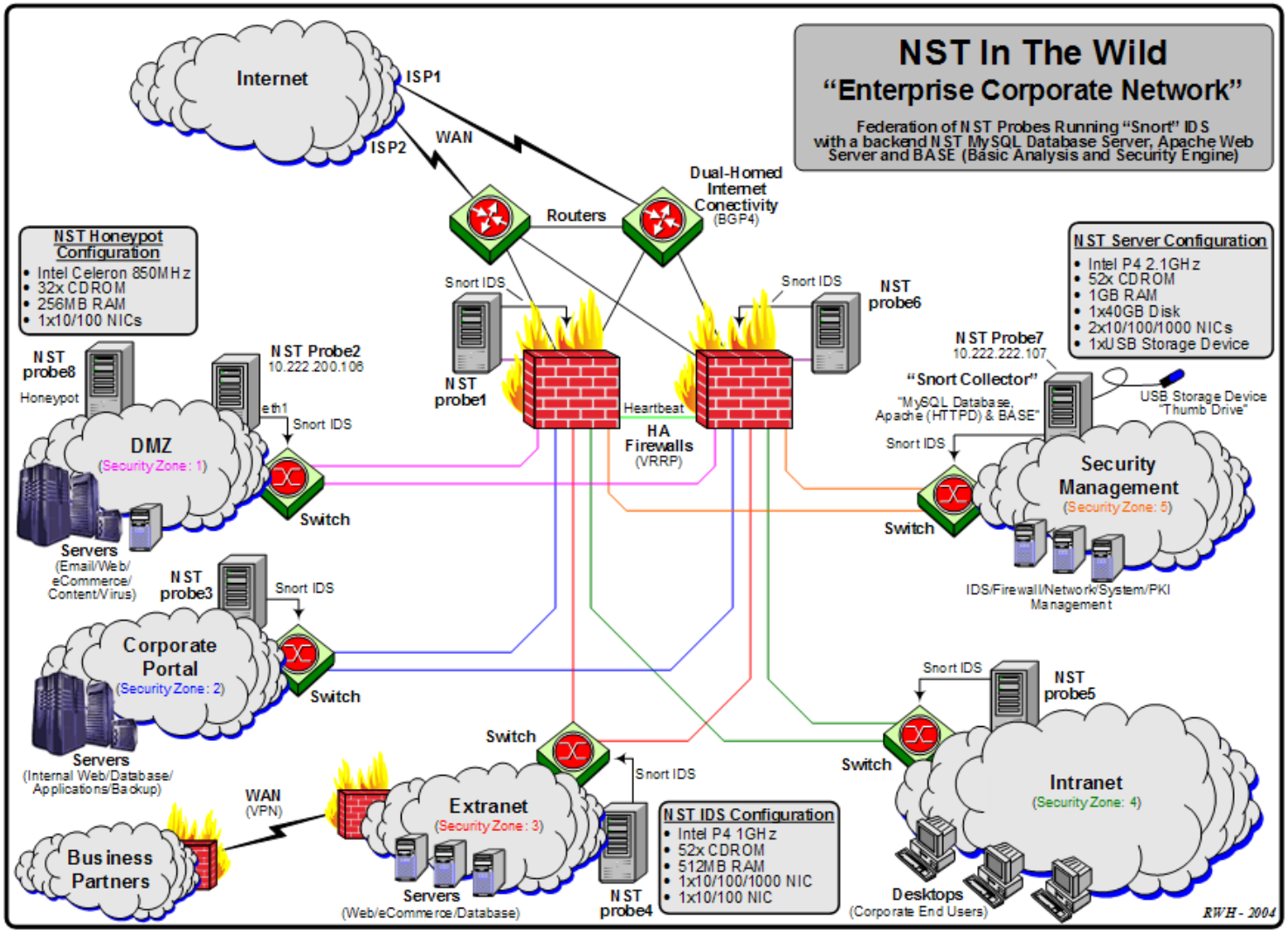
Enterprise Network

- An enterprise network is an enterprise communications backbone that helps connect computers and related devices across departments and workgroup networks, facilitating insight and data accessibility.
- An enterprise network reduces communication protocols, facilitating system and device interoperability, as well as improved internal and external enterprise data management.
- An enterprise network is also known as a corporate network.

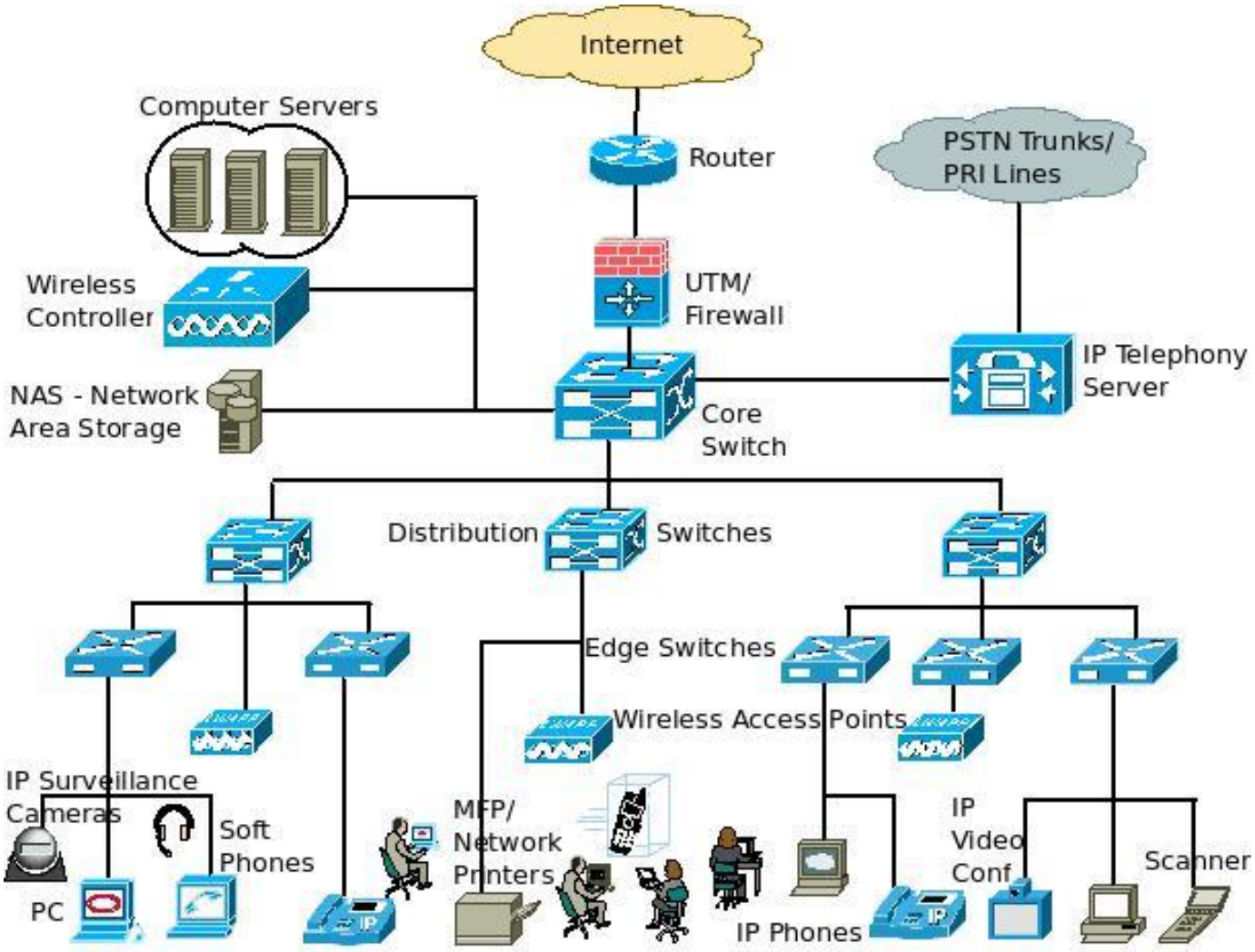
Examples of Enterprise IT Network



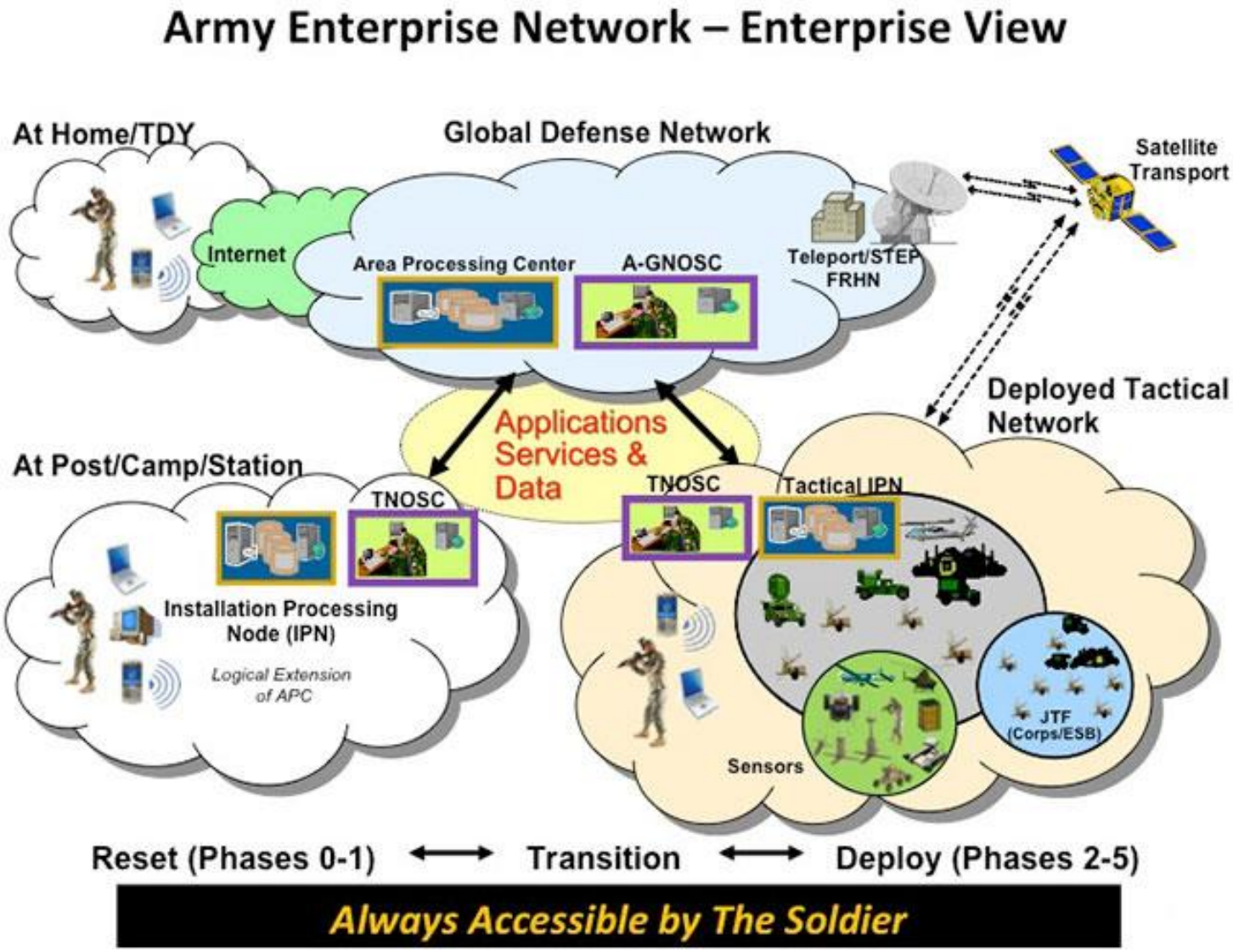
Examples of Enterprise IT Network



Examples of Enterprise IT Network



Examples of Enterprise IT Network



Need for Operations Security (Why)

- Increasing reliance on critical IT services.
  - Failure of these services cannot be acceptable.
- Increasing costs of IT systems failure.
  - Systems evolve to a more complicated form over time. Hence, costs of system failure will be increased.
- Increasing scale of users, malware and attacks.
  - Threats are constantly present and growing due to automated tools.

Operations Security Process (How)

1. Identify critical assets
   - E.g. IT systems, cash, employees
2. Analyse threats
   - E.g. Hackers, flood, power outage
3. Analyse vulnerabilities
   - E.g. Unpatched systems, residing in low lying areas
4. Assess risks
   - E.g. Frequent patches, low probability of flood
5. Employ protective measures
   - E.g. Patch management lifecycle, flood gantries

1. Identify Critical Assets

- What are they?
  - Assets that impacts critical business operations.
  - Quantify the impact to operations in terms of $$.
- How are they critical?
  - Link these assets to business operations and determine how it impacts operations if these assets are compromised.
  - Consolidate these assets and ranking them in order.
  - Subsequent steps will apply company's limited resources to protect important areas (assets) in terms of ranking order.

2. Analyze Threats

- What are threats?
  - Factors (mostly **external**) that may harm assets.
- How are threats analysed?
  - Make a list of potential activities/events that may cause disruption/damage to your assets.
  - Examine natural and man-made threats.
  - Used in later stage of assessing risks.

3. Analyze Vulnerabilities

- What are vulnerabilities?
  - Weaknesses (mostly **internal**) present in the assets.
- How are vulnerabilities analyzed?
  - Examine vulnerabilities in each critical asset.
  - No need to rectify yet as there may not be threats that can currently exploit these weaknesses.
  - Used in later stage of assessing risks.

4. Assess Risks

- What is Risk Assessment?
  - Risk = Threat x Vulnerability x Impact
  - Risk is the likelihood that a threat will exploit an asset's vulnerability causing impact to business.
- How are Risks Assessed?
  - Compute the risk for each possible threat-vulnerability-(asset) impact combination.
  - Prioritise the list so that action can be taken for high risk items.

5. Employ Protective Measures

- What are Protective Measures?
  - Ways to reduce or remove the risks identified.
- How are Measures Deployed?
  - Examine the threat, vulnerability and impact and think of ways to remove/reduce one or more.
  - Can be procedural or technological in nature.
  - Depends on limited resources vs. risk level.
    - Can employ more than one measure to reduce the same risk; can cover even low risk items.

Operations Security Process (Example)

Process	Example 1	Example 2
Identify Critical Assets	IT systems for online business (High)	IT systems for online business (High)
Analyse Threats	Hackers (High)	Power outage (Low)
Analyse Vulnerabilities	Weaknesses in IT system if patching not done on time (High)	Systems cannot function without power (High)
Assess Risks	High x High x High	High x Low x High
Employ Protective Measures	• Adopt patch management cycle • Operate an alternate system	• Standby backup power supply • Operate from an alternate site

Key Focus Areas in Operations Security (What)

1. Protecting valuable assets
2. Managing security services effectively
3. Maintaining operational resilience
4. Controlling privileged accounts

1. Protecting Valuable Assets

- Need to identify valuable assets.
- Protecting physical assets.
  - Facilities, hardware, software & media
- Protecting information assets.
  - Classify information according to confidentiality, integrity and availability requirements
- Cost of protecting must commensurate with the value of the assets.

2. Managing Security Services Effectively

- Focus: how are security technologies managed and used in the organization.
- Security measurements, metrics and reporting
  - E.g. firewall logs, firewall uptime=100%, perimeter security report
- Managing security technologies
  - E.g. malware defence, monitoring/reporting services, IDS/IPS, vulnerability management etc
- Key operational processes and procedures
  - E.g. change management, configuration management, patch management, incident management etc

3. Maintaining Operational Resilience

- Resilience – ability to recover from or adjust easily to misfortune or change.
- Understand common threats that our IT systems face and prepare for them.
  - Unauthorized disclosure (!Confidentiality)
  - Corruption and improper modification (!Integrity)
  - Destruction, interruption and theft (!Availability)
- Design and build systems to be resilient against these 3 threats or fail to a safe state.

4. Controlling Privileged Accounts

- Accounts: means for users to access IT systems.
  - E.g. Root /built-in admin, service, admin, power users, ordinary users accounts.
- Roles: specific job functions in the organization.
  - E.g. System admin, operators, security admin help desk personnel, ordinary users.
- How to control?
  - Assign accounts and privileges appropriately.
  - Review periodically for inactivity.
  - Ensure users have proper level of clearance.

What we will cover

- Focus: design, implementation, operation and management of enterprise IT systems.
- Operations security risk management process is covered in IT2522. This module will focus on the mitigating procedures.

What we will cover

1. Managing security services effectively
   - Malware defence and mgmt
   - Patch mgmt
   - Configuration mgmt
   - Security configuration mgmt
2. Maintaining operational resilience
   - Backup and recovery
   - Business Continuity Planning
   - InfoSec continuous monitoring
3. Controlling privileged accounts
   - User account mgmt
   - Personnel mgmt
   - MSSP (Outsourcing mgmt)

Conclusion

- Operations Security is about identifying threats, vulnerabilities and mitigating risks to ensure that business services can operate reliably.
- Need to focus resources where the need is the highest → risk management.

Summary

- What is Operations Security?
  - What are enterprise networks?
- Need for Operations Security
- Operations Security Process
- Key Areas of Operations Security