SWINBURNE
UNIVERSITY OF
TECHNOLOGY

Network Security and Resilience

Security Management

Lecture seven

Outline of Lecture

- Goals and competing priorities of security management
- Security definitions
- The need for a security programme
- ISO 27002 security programme framework
- Cisco security programme framework

Learning objectives

- At the end of this lecture you should be able to:
  - Describe some of the competing priorities that a security programme must address
  - Explain the following important security terms
    - Threat agent
    - Threat
    - Vulnerability
    - Risk
    - Exposure
    - Countermeasure
  - Describe the ISO27002 and Cisco security frameworks
  - Explain what the ‘Security Wheel’ is

Security Management Responsibilities

- Risk management
- Information security policies
- Procedures
- Standards
- Guidelines
- Baselines
- Information classification
- Security organisation
- Security education

Security Management

- It is not possible to guarantee 100% confidentiality, 100% integrity and 100% availability
  - Too expensive
  - Too many threats to be countered
  - Not always necessary
- Expense
  - Can guarantee 100 % confidentiality if communications transmitted over separate physical infrastructure but very expensive
- Too many threats
  - New threats evolve all the time
  - Best approach is to minimize the exposure to them and have mechanisms to detect new ones quickly
- Not always necessary to have 100% security
  - Depends on the business and the nature of the communication

Example

- University
  - Student emails
    - Probably moderate confidentiality, moderate integrity, moderate availability
  - Staff emails
    - Probably moderate, moderate and high
  - Depends on definition of levels of security and nature of communication
- Security management aims to manage risk
  - Areas of greatest risk are subject to more controls than areas of less risk
  - Need to have some way of quantifying risk

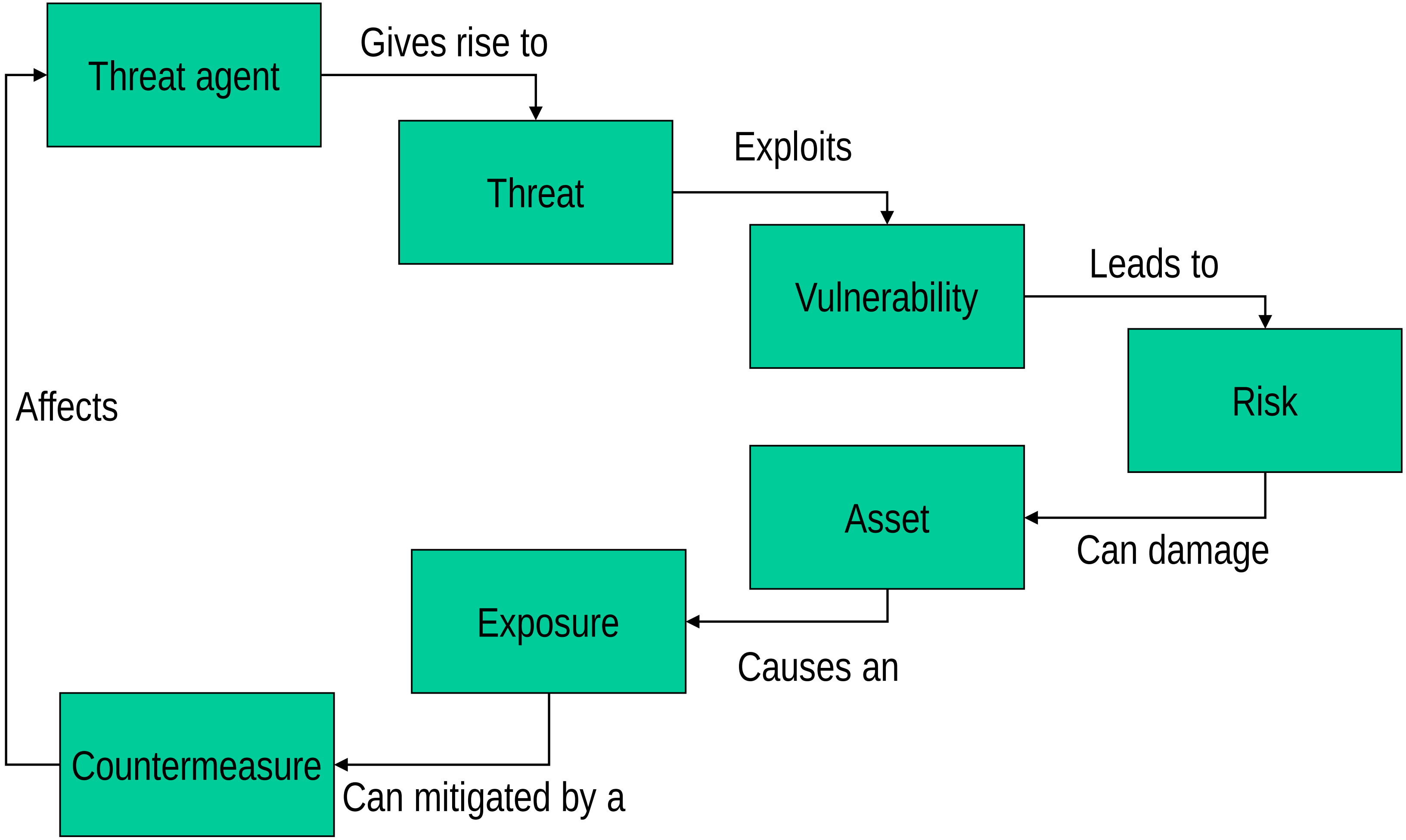
Security principles

- Need to have some measure of the difference aspects of Network Security required for the organisation
  - Confidentiality
    - Communication channels are kept secret
  - Integrity
    - Communications are unchanged
  - Availability
    - Communications services are available

Security definitions

- Vulnerability
  - A weakness in software, hardware or procedures that may provide an opportunity for attack
- Threat
  - Any potential danger to information or systems
- Risk
  - Likelihood of a threat agent exploiting a threat
- Exposure
  - An instance of being exposed to losses from a threat agent
- Countermeasure
  - A way of mitigating risk

Security definitions (Harris, 2012)



Types of countermeasures

- Administrative controls
  - Policies, standards, procedures, guidelines, screening of personnel, training, change control
- Technical controls
  - Access control mechanisms, passwords, resource management, authentication systems, security devices, network configuration
- Physical controls
  - Physical access, locking systems, monitoring systems, environmental controls, perimeter controls

Organisational security goals

- Countermeasures chosen depends on security goals
  - Stated in the security policy
- Need to distinguish between different types of security goals
  - Operational
    - Short term, days
    - Eg ensure network is protected from worm attacks
  - Tactical
    - Mid term, weeks
    - Eg Improve central control of hosts
  - Strategic
    - Long term, months
    - Move to a VPN based on IPSec

Security programme

- Many different aspects need consideration in securing an organisation's networking infrastructure
  - Threats, time horizons, appropriate controls
- Security needs to be implemented in a coherent and structured way
- The approach is to develop a security programme
  - Composed of policies, standards, baselines, guidelines and procedures
  - Most common framework for a security programme is the ISO 27002 standard

Security programme

- ISO 27002 identifies twelve main areas of security
  - Risk assessment
  - Management support for security
  - Organisational security
  - Asset classification and control
  - Personnel security
  - Physical and environmental security
  - Communications and operations management
  - Access control
  - Systems development and maintenance
  - Incident management
  - Business continuity planning
  - Compliance

Security programme

- There is no one generic security programme
- Has to be tailored to the specific enterprise
  - Each enterprise will have its own priorities that will be reflected in the security policy
  - E.g. A business that uses a web interface for a large transaction volume will have different requirements to one which has only occasional sales of high value products
  - Both may be web based companies and both have similar revenues
- ISO27002 and other security models provide a framework that can be used for the individual organisation

Information security policy

- The security policy will usually have a statement of management intent to support information security and some compliance requirements of staff
- The security policy should be readily available to members in the organisation
    - Some material may be sensitive but there should be a readily available outline with reference to sensitive material
    - It is not something to be done and then forgotten about

Organisational security

- Organisational security specifies how information security is managed within the organisation
  - Specifies who is responsible for what
    - Who is responsible for implementing network security?
    - Who is responsible for reporting security incidents?
    - Who is responsible for responding to security incidents?
    - What if the incident happens over Christmas when most people are on holiday?
    - …and similar questions…
  - There should be one manager with responsibility for all security related activities.
  - It should be very clear who that person is

Organisational security

- There should be regular reviews of the security policy implementation
  - Ensure that latest threats are dealt with
  - Ensure that procedures derived from policy work
- There should be regular contact with external bodies as to security obligations
  - Law enforcement agencies (eg. AFP, ASIO)
  - Regulatory bodies (eg. Australian Communications Authority)

Risk assessment

- There should be regular assessment of the risk environment of the organisation
  - Need to be aware of threats
  - Need to consider whether or not policy addresses them
  - Need to consider whether implementation of policy addresses them
- Risk should be assessed in a consistent manner, across the whole organisation
- Important that all functions of the organisation are considered for the risk they present to the functioning of the organisation

Asset classification and control

- You need to know what assets you have and what their importance is and who is responsible for them
  - information assets
    - databases in particular but also user documentation, training material, procedures, archives, disaster recovery plans
  - software assets
    - application software developed in-house, system software, development tools
  - physical assets
    - computers, networking infrastructure, accomodation
  - services
    - computing and communication services

Asset classification and control

- All major assets should be identified
- All should have a nominated owner
  - someone who knows what the asset does and what the consequences are if it is destroyed, stolen or compromised
  - this responsibility should be able to be delegated to someone else if the nominated owner is absent
  - The owner is responsible for the asset being maintained
    - maybe delegated

Information assets

- All information assets need to be classified so that they receive an adequate level of protection
  - sensitivity and criticality
  - need for sharing and protection of information asset
- Generally need to classify information assets in terms of
  - confidentiality, integrity and availability
- Need specific guidelines for the following situations
  - copying, storage, transmission by email, transmission by voice and destruction guidelines
- Examples
  - internal network structure including hostnames and addresses
  - customer lists, bank account details, sales lists

Personnel security

- Security in job definition and resourcing
  - adequate screening of potential recruits for sensitive positions
    - check references, CV details, claimed qualifications and identity
  - Needs to be extended to 3rd parties
- Training
  - employees should have regular training in security issues appropriate to their work
    - policies, procedures, systems, legal requirements, threats

Personnel security

- Responding to security incidents and malfunctions
  - There needs to be well defined procedures for dealing with incidents
- Reporting security incidents
  - Everyone must know what their role is and who it is delegated to when they are absent
- Reporting security weaknesses
- Reporting system malfunctions
- Learning from incidents
- Disciplinary process

Physical and environmental security

- Physical security perimeter
  - a barrier access through which requires some authorisation
    - card, occupied reception etc
  - Might be used to secure networking equipment or system servers
  - Needs to be physically secure
  - People within the security perimeter should wear some kind of identification
- How secure does the physical perimeter have to be?
  - how secure depends on what the perimeter protects
  - One extreme
    - Faraday cage with armed guards at the door and some biometric identification systems
  - Other extreme
    - Lock on the door and a few system passwords

Physical and environmental security

- Equipment security
  - protect from environment threats and physical attacks
  - Siting of equipment
    - eg don’t have the network server room next to a blast furnace
  - Things to consider with equipment security
    - theft, fire, explosives, smoke, water, dust, vibration, corrosive chemicals, electrical supply, e-m radiation
  - neighbourhood needs to be considered
    - what happens if the building next door catches fire?
  - Power supplies
  - cabling security and redundancy
  - laptops with sensitive information

Communications and operations management

- Operational procedures
  - Well defined and documented operating procedures
  - Operational change control
  - Incident management procedures
  - Segregation of duties
  - Separation of development and operational facilities
  - External facilities management

Communications and operations management

- System and network planning
  - Capacity
  - System and network testing
- Protection against malicious software
- Integrity
  - backups, operator logs, fault logs
- Network management
  - separation from computer operations
  - remote users
  - encryption

Communications and operations management

- Media handling and security
  - Removable media
  - Disposal of media
  - Information handling procedures
  - Security of network and system documentation
- Exchanges of information
  - Security of data in transit
  - eCommerce security
  - Email security
    - vulnerabilities, guidelines for use
  - Other information exchange mechanisms
    - video, voice, fax

Access control

- Control access to information
  - Some guiding policy needs to be established
    - only those who have a legitimate need to use information should have access to it
- User access management
  - registration procedures
  - appropriate privileges
  - password management
  - regular review of access privileges
- User responsibilities
  - passwords, unattended equipment

Access control

- Network access control
  - enforced path?
    - Do we specify that communications must be through a particular telco
  - authentication for remote users
    - Multi-factor?
  - node authentication
    - Can any device connect to the network?
  - remote diagnostics
    - How is trouble shooting carried out?
  - virtual networks
    - What processes are in place for establishing VPNs?
  - services (eg how do people access email, how do they connect remotely?)

Access control

- Operating system accesses
  - record accesses, including failed accesses
  - connection time restrictions
  - identification
  - timeouts
  - duress alarms
- Application access control
  - information access restrictions
  - sensitive system isolation
  - Monitoring system access and use
  - Mobile computing and remote use

Systems development and maintenance

- New systems will have security requirements
  - eg. data validation
    - particularly important for preventing buffer overflow attacks
- Cryptographic controls
- File system security
- Development process security
- Covert channels and trojan code
- Third party software development

Business continuity management

- To protect critical business processes from the effects of major failures or disasters
- Includes “Disaster Recovery”
  - But a lot more than that
    - E.g. our ISP has a massive failure
    - Or there is a fire in our server room
- Need to identify risks and understand the consequences
- Need to prepare the Continuity Plan

Business continuity management

- How the plan is activated
- Emergency procedures
  - contacting police, ambulance, fire service, local government etc
- Fallback procedures for moving business activities to alternative locations
- Resumption procedures
- Testing of Business Continuity plan
- Responsibilities of individuals and their alternatives

Incident investigation

- There should be a well established procedure for
  - Investigating security incidents
  - Learning from them
- “Learning” means the organisation puts in place strategies for ensuring the incidents do not recur or, if that is not possible, minimising damage when they do occur

Compliance

- Avoiding breaches of law
- Identification of relevant law
- Safeguarding organisational records
- Data protection
- Prevention of misuse of facilities
- Collection of evidence
- Reviews of security policy
- System audits

Cisco security model

- Cisco's security model is approximately a subset of the ISO 27002 model
- It is concerned (primarily) with the network related aspects of security management
- Cisco identify the following four broad areas that need to be addressed in a security programme
  - Host security
  - Network security
  - Organisational security
  - Legal security

Cisco security model

- Host security
  - How to authenticate users
  - How to control access to system resources
  - How to store and process data within the system in a secure way
  - How to construct audit trails
  - For each of these topics confidentiality, integrity and availability has to be considered
- Network security
  - How to control access to computer networks and distributed systems
  - How to transmit data between hosts maintaining
    - Confidentiality
    - Integrity
    - Availability

Cisco security model

- Organisational security
  - Technical solutions of themselves are inadequate for secure networks and systems
  - Most security problems are human
- Legal security
  - How to ensure that there are sufficient audit trails, procedures and the like to ensure that any legal action against us can be defended
  - Or we can take action against someone who has attacked us

Questions

- Using the Cisco model, what aspect of security policy covers the following events?
  - Virus protection software needs updating
  - We have been blamed for an email based denial of service attack coming from our machines. We have investigated the issue and believe that our email address was spoofed.
  - We have been blamed for an email based denial of service attack coming from our machines. We have investigated the issue and have confirmed that our hosts were compromised and did launch the attack.

Security 'wheel'

- Security policy has many components
  - often difficult to get right first time
    - balance between security and usability
    - issues not adequately dealt with
    - new problems
- Security policy needs continuous review and, once implemented, continuous monitoring of effectiveness
- Process of review and monitoring sometimes referred to as the 'security wheel'
  - Secure
  - Monitor
  - Test
  - Improve

Conclusion

- Security policy enables an organisation to make decisions in a structured way as to the necessary confidentiality, integrity and availability needed for different activities of the organization
- Our interest in this unit is mostly in Communications and Operations Management, and Access Control but you need to have an appreciation of all aspects of security
- Being 100% risk free is not possible
  - too expensive in terms of money, time, people and effort to eliminate all risk
  - there will always be some risk
- The security programme is concerned with identifying what level of risk is acceptable and how to manage that risk