LECTURE 3
COMPUTER SECURITY AUDIT ANALYSIS

Implementing IT Security Management

- We continue the examination of IT security management, exploring the range of management, operational and technical controls or safeguards available that can be used to improve security of IT systems and processes.

- We then explore the content of the security plans that detail the implementation process.

-

- These plans must then be implemented, with training to ensure all personnel know their responsibilities, and monitoring to ensure compliance.

- Finally, to ensure that a suitable level of security is maintained, management must follow up the implementation to evaluate the effectiveness of the security controls and to iterate the entire IT security management process.

INFORMATION SECURITY ~~AUDIT~~, PLAN, PROTECTION, CONTROL, ~~DESIGN~~

INFORMATION SECURITY PLAN,

IT Security Plan

- Having identified a range of possible controls, from which management have selected some to implement, an IT security plan should then be created.
- This is a document that provides details as to what will done, what resources are needed, and who will be responsible.
- The goal is to detail the actions needed to improve the identified deficiencies in the organization's risk profile in a timely manner

IT Security Plan

- Suggests that this plan should include details of:
  - risks (asset/threat/vulnerability combinations)
  - recommended controls (from the risk assessment)
  - action priority for each risk
  - selected controls (on the basis of the cost-benefit analysis)
  - required resources for implementing the selected controls
  - responsible personnel
  - target start and end dates for implementation
  - maintenance requirements and other comments

Implementation Plan

Risk (Asset/Threat)	Level of Risk	Recommended Controls	Priority	Selected Controls	Required Resources	Responsible Persons	Start - End Date	Other Comments
Hacker attack on Internet Router	High	1. disable external telnet access 2. use detailed auditing of privileged command use 3. set policy for strong admin passwords 4. set backup strategy for router config file 5. set change control policy for the router configuration	1	1. 2. 3. 4. 5.	1. 3 days IT net admin time to change & verify router config, write policies; 2. 1 day of training for net admin staff	John Doe, Lead Network Sys Admin, Corporate IT Support Team	1-Feb-2006 to 4-Feb-2006	1. need periodic test & review of config & policy use

Security Plan Implementation

- plan documents what is required
- identified personnel perform needed tasks
  - to implement new or enhanced controls
  - may need upgrades or new system installation
  - or development of new/extended procedures
  - need support from management
- monitored to ensure process correct
- when completed management approves

Implementation Follow-up

- security management is cyclic, repeated
- need to monitor implemented controls
- evaluate changes for security implications
  - otherwise increase chance of security breach
- have a number of aspects, which may indicate need for changes in previous stages of process

Implementation Follow-up

- need continued maintenance and monitoring
  - to ensure continued correct functioning and appropriateness
- tasks include:
  - periodic review of controls
  - upgrade of controls to meet new requirements
  - check system changes do not impact controls
  - address new threats or vulnerabilities
- goal to ensure controls perform as intended

INFORMATION SECURITY PROTECTION & DETECTION

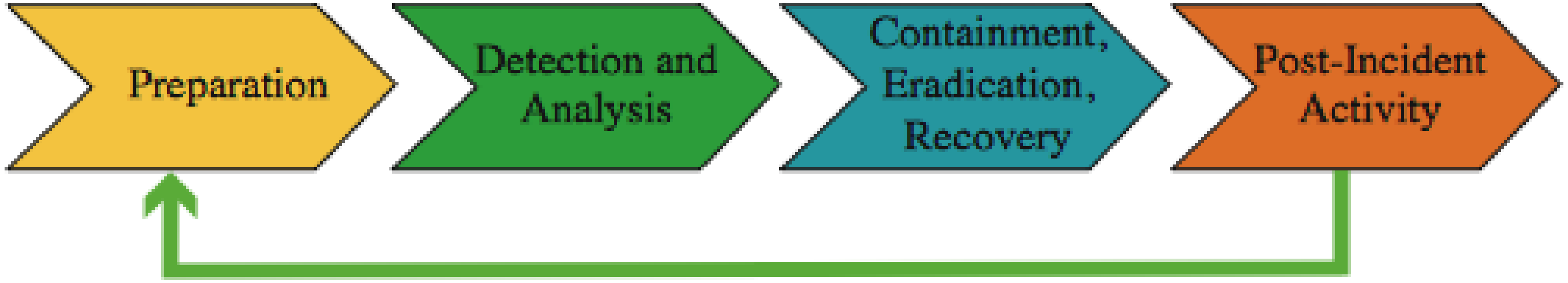
Detecting Incidents

- reports from users or admin staff
  - train and encourage such reporting
- detected by automated tools
  - e.g. system integrity verification tools, log analysis tools, network and host intrusion detection systems, intrusion prevention systems
  - updated to reflect new attacks or vulnerabilities
- admins must monitor vulnerability reports

Type of Security Incidents

- any action threatening classic security services
- unauthorized access to a system
  - unauthorized viewing by self/other of information
  - bypassing access controls
  - using another user’s access
  - denying access to another user
- unauthorized modification of info on a system
  - corrupting information
  - changing information without authorization
  - unauthorized processing of information

Managing Security Incidents



Managing security incidents involves procedures and controls which address:

- detecting potential security incidents
- identifying and responding to breaches in security
- documenting breaches in security for future reference

Information learnt as a result of a security incident should be used to improve procedures and the risk profile in the future.

Responding To Incidents

- need documented response procedures
- procedures should
  - identify typical categories of incidents and approach taken to respond
  - identify management personnel responsible for making critical decisions and their contacts
  - whether to report incident to police/CERT etc

Documenting Incidents

- need to identify vulnerability used
  - how to prevent it occurring in future
- recorded details for future reference
- consider impact on org and risk profile
  - may simply be unlucky
  - more likely risk profile has changed
  - hence risk assessment needs reviewing
  - followed by reviewing controls in use

INFORMATION SECURITY CONTROL

What is Security Control or Safeguard

- Given the results of some form of risk assessment on an organization's IT systems which identify areas needing treatment, the next step is to select suitable controls to use in this treatment.
- IT security controls or safeguards (the two terms are used interchangeably) help to reduce risks.
- Some controls can serve to address multiple risks at the same time, and selecting such controls can be very cost effective.

What is Security Control or Safeguard

- Controls can be classified as belonging to one of the following classes (although some controls include features from several of these):

management control

- Focus on security policies, planning, guidelines and standards which then influence the selection of operational and technical controls to reduce the risk of loss and to protect the organization’s mission.
- These controls refer to issues that management needs to address.

What is Security Control or Safeguard

Operational

- Address the correct implementation and use of security policies and standards, ensuring consistency in security operations, and correcting identified operational deficiencies.

- These controls relate to mechanisms and procedures that are primarily implemented by people rather than systems. They are used to improve the security of a system or group of systems.

Technical controls

- **I**nvolve the correct use of hardware and software security capabilities in systems. These range from simple to complex measures that work together to secure critical and sensitive data, information, and IT systems functions.

Technical Control

- **Supportive**: generic, underlying technical IT capabilities
- **Preventative**: focus on preventing security breaches by warning of violations
- **Detection/recovery**: focus on response to a security breach

List of Control

CLASS	CONTROL FAMILY
Management	Risk Assessment
Management	Planning
Management	System and Services Acquisition
Management	Certification, Accreditation, and Security Assessments
Operational	Personnel Security
Operational	Physical and Environmental Protection
Operational	Contingency Planning
Operational	Configuration Management
Operational	Maintenance
Operational	System and Information Integrity
Operational	Media Protection
Operational	Incident Response
Operational	Awareness and Training
Technical	Identification and Authentication
Technical	Access Control
Technical	Audit and Accountability
Technical	System and Communications Protection

Cost-benefit Analysis

- It is likely that the organization will not have the resources to implement all the recommended controls.
- Therefore, management should conduct a cost-benefit analysis to identify which controls are most appropriate and provide the greatest benefit to the organization given the available resources.
- This analysis may be qualitative or quantitative, and must demonstrate that the cost of implementing a given control is justified by the reduction in level of risk to assets that it provides.

Cost-benefit Analysis

- It should include details of the impact of implementing the new or enhanced control, the impact of not implementing it, and the estimated costs of implementation.

- It must then assess the implementation costs and benefits against system and data criticality to determine the importance of choosing this control.

- Management must then determine which selection of controls provides an acceptable resulting level of risk to the organization’s systems.

Cost-benefit Analysis

- This selection will consider factors if the control:

  - ✓ reduces risk more than needed, then a less expensive alternative could be used
  - ✓ cost more than the risk reduction provided, then an alternative should be used
  - ✓ not reduce the risk sufficiently, then either more or different controls should be used
  - ✓ provides sufficient risk reduction, and is the most cost effective, then use it.

Cost-benefit Analysis

- It is often the case that the cost of implementing a control is more tangible and easily specified than the cost of not implementing it.
- Management must make a business decision regarding these ill-defined costs in choosing the final selection of controls and resulting residual risk.

Roadmap/Mind Map