ACS-2821-001
Information Security in Business

Operations Security

ACS-2821-001 – Slides Used In The Course

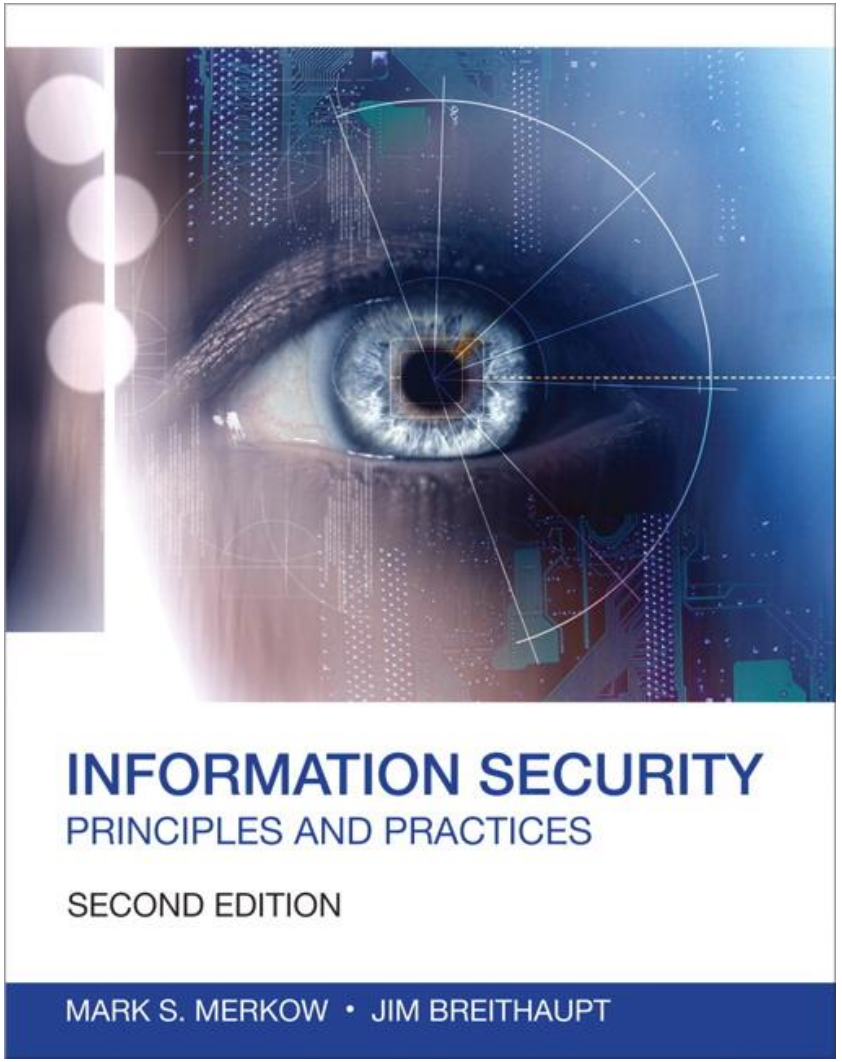
THE UNIVERSITY OF WINNIPEG

A note on the use of these slides:

These slides has been adopted and/or modified from the original for the use in this course. The author of the text have make these slides available to all (faculty, students, readers) and they obviously represent a *lot* of work on their part.

In return for use, please:

- If slides are being used (e.g., in a class) that the source be mentioned (after all, the author like people to use our book!)
- If any slides are being posted on a www site, note that they are adapted from (or perhaps identical to) the author original slides, and note their copyright of this material.



Objectives

- Outline the types of controls needed for secure operations of a data center
- Explain the principle of least privilege
- Differentiate between the principle of least privilege and the principle of separation of duties
- Define the control mechanisms commonly found in data center operations
- Create a model of controls that incorporate people, process, and technology-based control mechanisms

What is Operations Security

- Operations security is used to identify the controls over software, hardware, media, and the operators and administrators who possess elevated access privileges to any of these resources
- The primary focus is on data center operations processes, people, and technology
- Specific types of controls are needed
  - ***Preventative controls*** reduce the frequency and impact of errors and prevent unauthorized intruders
  - ***Detective controls*** discover errors after they occur
  - ***Corrective or recovery controls*** help mitigate the impact of a loss
  - ***Deterrent controls*** encourage compliance with external controls
  - ***Application-level controls*** minimize and detect software operational irregularities
  - ***Transaction-level controls*** provide control over various stages of a transaction

Operations Security Principles

- Principle of least privilege (need-to-know)
  - Defines a minimum set of access rights or privileges needed to perform a specific job description
  - *E.g. military or law enforcement agency*
- Separation of duties
  - A type of control that shows up in most security processes to make certain that no single person has excessive privileges
  - *E.g. double custody*

Operations Security Principles

- Two fundamental reasons behind Separation of duties
  - People are an integral part of every operations process. They authorize, generate, and approve all work that's needed.
  - People have shortcomings. When individuals perform complementary checks on each other, there is an opportunity for someone to catch an error before a process is fully executed
  - *E.g. two signature is require to sign on any legal documents*

Operations Security Process Controls

Necessary to secure data center operations

- Trusted recovery controls
  - Ensure that security is not breached when a computer system crashes
  - *E.g. BCP and DRP processes*
- Configuration and Change Management controls
  - Used for tracking and approving changes to a system
  - *E.g. patch management*
- Personnel security
  - Involves pre-employment screening and mandatory vacation time
  - *E.g. background check, security clearance, references and etc.*

Operations Security Process Controls

- Record retention processes
  - Refers to how long transactions and other types of computerized or process records should be retained
  - *E.g. event logs, transaction logs, backup rotation and etc.*
- Resource protection
  - Protects company resources and assets
  - E.g. physical and logical security control
- Privileged entity controls
  - Given to operators and system administrators as special access to computing resources
  - *E.g. backup operators vs domain administrators*
- Media viability controls
  - Needed for the proper marking and handling of assets
  - *E.g. backup media, onsite storage vs offsite storage*

Operations Security Controls in Action

- The principles needed for secure operation of data center assets
  - Software support
  - Configuration and change management
  - Backups
  - Media controls
  - Documentation
  - Maintenance
  - Interdependencies

Operations Security Controls in Action

- Software support
  - It's essential that software functions correctly and is protected from corruption
  - Several elements of control are needed
    - Limiting what software is used on a given system
    - Inspecting or testing software before it is loaded
    - Ensuring software is properly licensed
    - Ensuring software is not modified without proper authorization

Operations Security Controls in Action

- Configuration and Change management
  - To ensure that users don't cause unintentional changes to the system that could diminish security
  - To ensure that changes to the system are reflected in up-to-date documentation, such as the contingency or continuity plan

Operations Security Controls in Action

- Backups
  - This function is critical to contingency planning
  - Backups should be stored securely and preferably at a different site, in case the building where the computing equipment is located is inaccessible

Operations Security Controls in Action

- Media controls
  - Include a variety of measures to provide physical and environmental protection and accountability for tapes, optical media, USB (Flash) drives, printouts, and other media
    - Common media controls
    - Marking
    - Logging
    - Integrity verification
    - Physical access protection
    - Environmental protection
    - Transmittal
    - Disposition

Operations Security Controls in Action

- Documentation
  - Documentation of all aspects of computer support and operations is important to ensure continuity and consistency
  - Security documentation and procedures manual should be written to inform system users how to do their jobs securely

Operations Security Controls in Action

- Maintenance
  - System maintenance requires either physical or logical access to the system
  - Maintenance may be performed on site, or it may be necessary to move equipment to a repair site
  - Maintenance may also be performed remotely via communications connections
  - It may be necessary to take additional precautions such as conducting background investigations of service personnel

Operations Security Controls in Action

- Interdependencies
  - Support and operations components coexist in most computer security controls
  - These components are
    - Personnel
    - Incident handling
    - Contingency planning
    - Security awareness, training, and education
    - Physical and environmental
    - Technical controls
    - Assurance

Summary

- Operations security clarifies the controls needed to ensure secure data center operations
- The principle of least privilege, which limits operators' access rights or privileges, is essential to prevent abuses
- A clear separation of duties is necessary to prevent abuses at a transaction or business process level
- Controls ensuring the maintenance of the operation must also be present and operating successfully

ACS-2821-001 – Questions?