OPSEC & Production Controls

CSH6 Chapter 47

"Operations Security and Production Controls"

M. E. Kabay & Don Holden, and Myles Walsh

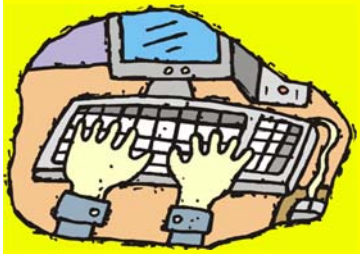
Copyright © 2015 M. E. Kabay. All rights reserved.

Topics in CSH6 Ch 47

- Introduction
- Operations Management
- Ensuring a Trusted Operating System
- Protection of Data
- Data Validation

Copyright © 2015 M. E. K

Introduction

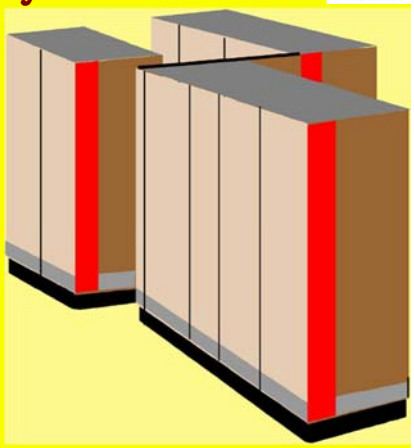


- *Production system* – one upon which enterprise depends critically
- *Operations* – requirements for control, maintenance, support of production systems
- *Computer program* – a set of instructions that tells a computer what to do to perform a task
- *Procedures* – sets of statements that tell a computer what to do in certain situations
- *Data files* – files that store information

Copyright © 2015 M. E. Kabay. All rights reserved.

Production Systems

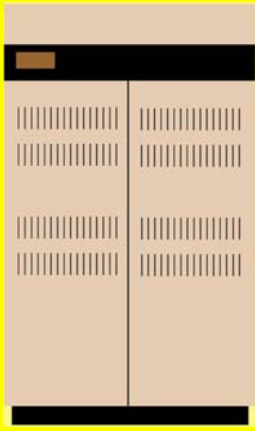
- Mission-critical
  - Essential
  - Required
  - Authorized
  - Official
- Contrast with:
  - Development
  - Test
  - Experimental
  - Personal



Copyright © 2015 M. E. Kabay. All rights reserved.

Operations

- Control
  - Integrating new programs
  - Running *jobs*
  - Managing access
- Maintenance
  - Updating versions
  - Running diagnostics
  - Doing backups
- Support
  - Responding to emergencies
  - Mounting required media
  - Managing networks



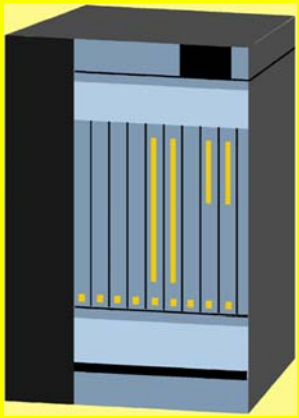
Copyright © 2015 M. E. Kabay. All rights reserved.

Computer Programs

- Stored instructions determining computer actions
- Sources
  - Internal – from *developers*
  - External – from *suppliers*
- Libraries of code
  - Source code
  - Executables (object code, load modules)
- Developers send code to *quality assurance* (QA)
- QA send approved code to *operations* (OPS)
- Changes to production code can be as *patches*

Copyright © 2015 M. E. Kabay. All rights reserved.

Procedures



- In general discussion:
  - Policy sets goals
  - Procedures define how to achieve goals
- In OPS,
  - Procedures may be specific automated routines
  - Batch systems use JCL to control sequence of program execution
    - ✓ Job Control Language (JCL) is a procedural language for controlling operations of computer
    - ✓ Can branch on conditions

Copyright © 2015 M. E. Kabay. All rights reserved.

Data Files

- OPS work with files
  - All operational data reside in *files*
  - Most modern system work with *databases*
- Some files are temporary (transient)
  - Work files created during jobs
  - Most production files are essential
    - ✓ Must be protected
      - Access-controls
      - Backups
- Log files keep records of system activity

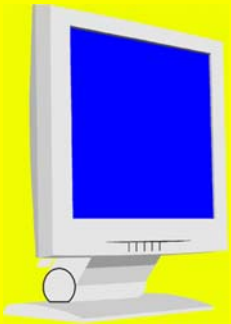
Copyright © 2015 M. E. Kabay. All rights reserved.

Operations Management

- Separation of Duties
- Security Officer / Administrator
- Limit Access to OPS Center
- Change-Control Procedures
- Externally-Supplied Software
- QC vs QA

Copyright © 2015 M. E. Kabay. All rights reserved.

Separation of Duties



- Applied to development and production of programs
- Operations staff participate in functional analysis and requirements definition phases
- Programmers modify code under development
- Managers sign off on updates
- OPS staff implement changes in production

Copyright © 2015 M. E. Kabay. All rights reserved.

Security Officer / Administrator

- Responsible for securing enterprise systems
- Applies security policies
- Modifies account privileges

Limit Access to OPS Center

- Need, NOT Status, determines access
- Identification and authentication for access
  - What one has
  - What one knows
  - What one is
  - What one does
- Log in and badge visitors
- Accompany visitors
  - No unaccompanied visitors
  - Not even to bathroom! (high-security)

Copyright © 2015 M. E. Kabay. All rights reserved.

Change-Control Procedures

- Moving new version of S/W to production
  - Identify software
  - Authorize change
  - Schedule update
  - Backup old data
  - Log update
  - Back out and recover older versions
- Using Digital Signatures to Validate Production Programs
  - Date, timestamp, checksum, keys

Copyright © 2015 M. E. Kabay. All rights reserved.

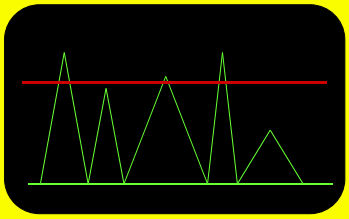
Externally-Supplied Software

- COTS software
  - Trojan Horses and Easter Eggs
  - Verify digital signatures of COTS
  - Compile from source when possible
- If resources allow, consider full QA testing
  - Verification of code execution using test-coverage monitors
- Open-source software pro/con
  - Full access to source code
  - May be many programmers improving code
  - But may be no technical support at all

Copyright © 2015 M. E. Kabay. All rights reserved.

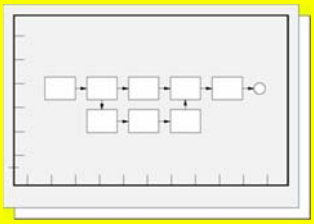
QC vs QA

- Definitions
- Service Level Agreements (SLAs)
- Monitoring Performance
- Monitoring Resources
- Monitoring Output Quality

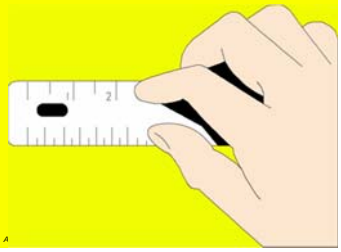


Copyright © 2015 M. E. Kabay. All rights reserved.

QA / QC Definitions



- QA: processes for ensuring and verifying validity of production programs
- QC: verifying quality of output



Copyright © 2015 M. E. Kabay. A

Service Level Agreements (SLAs)

- No absolute standard of quality for computing operations
- Define suitable balance of quality and cost
- Determine agreements on acceptable performance = SLAs
  - Performance
  - Resource utilization
  - Response time
    - ✓Not necessarily simple to define
- Use statistical measures
  - Confidence limits; e.g., "< x seconds in 95% of cases…"

Copyright © 2015 M. E. Kabay. All rights reserved.

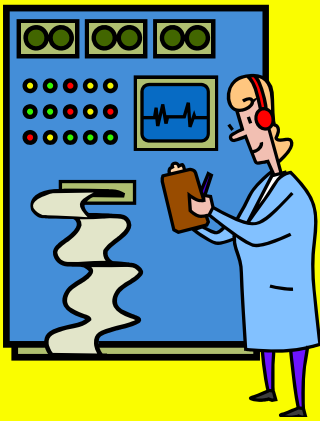
Monitoring Performance

- Computer-system performance depends on
  - CPU
  - DISK
  - RAM
  - Application design
- Network performance also depends on bandwidth and traffic
- Monitor performance constantly
  - Develop statistical base for spotting trends
  - Watch out for inflection points
  - Analyze outliers

Copyright © 2015 M. E. Kabay. All rights reserved.

Monitoring Resources

- Same principles of monitoring apply to resource utilization
- Must be capable of predicting resource exhaustion in advance
  - Take action to forestall disaster
  - E.g., reduce demand, increase efficiency or increase resources
  - Pay special attention to sudden changes and to outliers
- Chargeback systems help to increase user attention to resource utilization



Copyright © 2015 M. E. Kabay. All rights reserved.

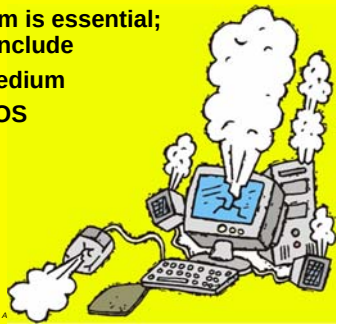
Monitoring Output Quality

- Always include meticulous attention to output quality
- Identify causes of problems and rectify them
- Keep track of error rates and be alert to increases

Copyright © 2015 M. E. Kabay. All rights reserved.

Ensuring a Trusted Operating System

- Trusted Computing Base (TCB) includes all aspects of system including hardware and software
- Trusted operating system is essential; methods of ensuring it include
  - Known-Good Boot Medium
  - New Versions of the OS
  - Patching the OS



Copyright © 2015 M. E. Kabay. A

Known-Good Boot Medium

- OS usually most expensive and important software on the production system
- Critically important to ensure that OPS have trustworthy, undamaged copy of OS at all times
- Especially important when applying changes (patches)
- Define "Known-Good" boot medium
  - Never exposed to possible corruption from other software
  - Copied from previous version of KG medium

Copyright © 2015 M. E. Kabay. All rights reserved.

New Versions of the OS

- Reinstall KG version of current OS before installing new OS version
- Create copy of KG version of new OS immediately
- Thus no other programs are run between time of installation and time of copy

Copyright © 2015 M. E. Kabay. All rights reserved.

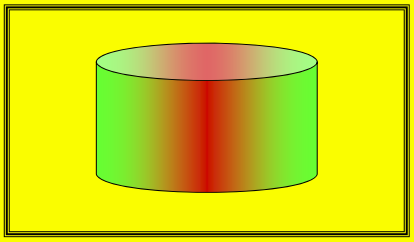
Patching the OS

- Patches make required changes to the OS
- Reinstall the KG version of the current OS
- Install the patches
- Make a copy of the patched OS at once to create the KG copy of the patched version

Copyright © 2015 M. E. Kabay. All rights reserved.

Protection of Data

- Access to Production Programs
- Separating Production / Development / Test Data
- Controlling User Access to Files & DBs



Copyright © 2015 M. E. Kabay. All rights reserved.

Access to Production Programs

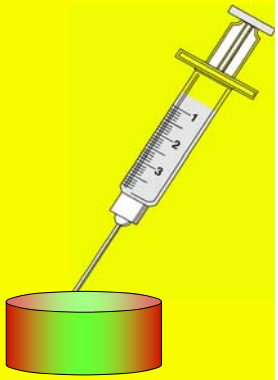
- Three classes of people need access
  - Users
  - Programmers
  - Operations staff

- Users access appropriate data through programs; they cannot modify production programs
- Programmers access *development* versions of programs and *test* data; they do not access production data except for purposes of repair
- OPS staff control and use production programs but do not access production *data* except for maintenance purposes (e.g., backups, diagnostics)

Copyright © 2015 M. E. Kabay. All rights reserved.

Separating Production / Development / Test Data

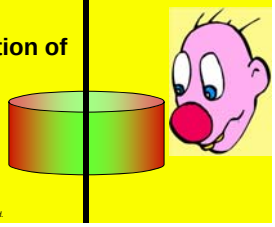
- Unacceptable to test programs using the production data files
  - Dangers of data integrity
  - Issues of confidentiality and privacy
  - Interference with availability for users
- Can extract sample data
  - Anonymize sensitive fields
- QA group can authorize transfer of programs between testing and production



Copyright © 2015 M. E. Kabay. All rights reserved.

Controlling User Access to Files & DBs

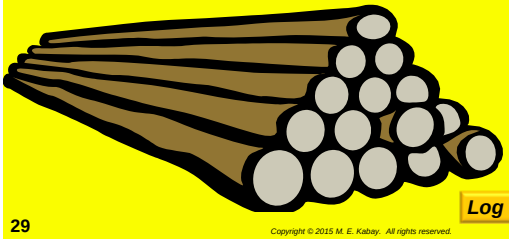
- Some information is confidential
  - Thus specific users may have access only to specific columns (attributes) or rows (instances) of the data
- Some files are auditable
  - Must keep accurate record of all transactions
  - Cannot allow any modification of sequence or content
  - E.g., general ledger



Copyright © 2015 M. E. Kabay. All rights reserved.

Data Validation

- Validation controls are normal part of OPS job
- Techniques include
  - Edit Checks
  - Check Digits & Log Files
  - Checks when Handling External Data



Log files

Copyright © 2015 M. E. Kabay. All rights reserved.

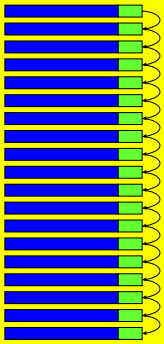
Edit Checks

- Many diagnostic programs available for file integrity checking
  - E.g., database programs check pointers
  - Identify orphaned records, broken chains
- Application systems include special diagnostics
  - Check business logic rules
  - E.g., verify that sum in order header matches total of extended prices in order detail

Copyright © 2015 M. E. Kabay. All rights reserved.

Check Digits & Log Files

- Generate *check digits* or *hash totals* based on contents of records during transactions
- Only authorized applications create proper cryptographic hash
  - Use public key cryptosystem for digital signatures
- Verify that records have correct check digits during diagnostic routines
  - Error indicates unauthorized change
- High security applications can use chaining
  - Each record calculates hash by including previous record's hash



Copyright © 2015 M. E. Kabay. All rights reserved.

Handling External Data

- Data can originate outside corporate control
- Use diagnostic procedures
  - Analyze data before accepting into production databases
  - Check business rules, integrity, safety
- Input of bad data can corrupt entire production system

Copyright © 2015 M. E. Kabay. All rights reserved.

Review Questions (1)

1. Give examples of production and non-production systems in
   a. A library
   b. A factory
   c. A hospital
2. Using reading and research if necessary, determine whether the following personnel are usually considered to be part of the operations group:
   a. Software developers
   b. Quality assurance personnel
   c. Computer operators
   d. System managers
   e. Network managers
   f. Information security officers

Copyright © 2015 M. E. Kabay. All rights reserved.

Review Questions (2)

3. Explain why a software engineer who has written the BigAccounting.EXE program and knows it inside out should no longer be able to change her own program once it has been moved into production.
4. Why does the President of Xyzcorp not normally have root access to the production system?
5. Why does it make sense to ensure that all visitors and staff wear badges at all times in a production environment? Why can't you just ensure that visitors wear badges?
6. Why can't the programmers simply install the new versions of their software into production libraries whenever the changes are complete?
7. How can digital signatures help to prevent problems in production code?

Copyright © 2015 M. E. Kabay. All rights reserved.

Review Questions (3)

8. What is an *Easter Egg*? What are the implications of finding Easter Eggs in production code from your shop?
9. What's an SLA and how does it fit into the Parkerian Hexad?
10. Why and how should one monitor computer performance from a security standpoint?
11. Why and how should one monitor computer resource utilization from a security standpoint?
12. What does it mean to "provide a known-good boot medium" and how does this bear on security?
13. How can *programmers* test their data effectively if they don't have full access to production data?
14. If *QA personnel* have access to samples of production data, how can confidentiality of private data be assured?

Copyright © 2015 M. E. Kabay. All rights reserved.

DISCUSSION

Copyright © 2015 M. E. Kabay. All rights reserved.