Security Management and Administration of Deployed Systems

Nelson Lee
Stephen Raio
Overview

• System Administrator role
• Acquisition Management
• Contracts and Service Level Agreements
• Problem Management
• Monitoring and Auditing
System Administrator Role

• NSTISSI No. 4013
• Defines a system administrator’s capability and responsibility
  – Work closely with the Information Systems Security Officer (ISSO) to ensure network is used securely
  – Participate in incident reporting
  – Maintain records of configuration controls in systems and applications
  – Advise ISSO of security anomalies and integrity loopholes
  – Administering user identification and authentication mechanisms
Required Technical Competencies

• General security policy
  – Able to define a local e-mail privacy policy
  – Identify information resource owner/custodian
  – Discuss integrity concepts
  – Explain LAN security as related to local policy
  – Describe workstation security policies

• General procedures
  – Practice and use facility management
  – Explain internet security procedures
  – Perform operating systems security procedure
Required Technical Competencies

• General Education, Training, and Awareness
  – Discuss the principle elements of security training
  – Discuss the objectives of security inspections/reviews
  – Identify different types of vulnerabilities

• Access Control Countermeasures
  – Define internal controls and security
  – Identify methods of intrusion detection
  – Define network firewalls

• Audit Policies
  – Summarize audit-related documentation
  – Use alarms, signals, and reports in accordance with existing policies and procedures
Required Technical Competencies

• Contingency preparations
  – Practice backups
  – Describe disaster recovery
  – Describe continuity planning

• Contingency configuration management
  – Practice change control
  – Explain database integrity
  – Perform management of media and tapes
  – Identify storage media protection and control procedures
Acquisition Management Process

• The need to outsource to 3rd party vendors
  – Includes responsibilities for:
    • Requesting
    • Evaluating
    • Acquiring
    • Managing
  – Information security requires cooperation with IT level
Acquisition Management Methods

• Formally managing acquisitions
  – Software Acquisition Capability Maturity Model (SA-CMM)

• OSD Acquisition Reform

• Evolutionary Acquisition
NSA/CSS Circular No. 500R

- Published in January 9, 2001
- Designed to optimize total system performance and minimize life-cycle costs
  - Based on risk, cost, performance, and schedule
  - Applies functional analysis, design synthesis, verification, system analysis and control
  - Recognizes the tradeoff between cost and performance
500R on Software Engineering

• Apply best practices
• Take advantage of open systems
• Use COTS
• Employ software reuse
• Apply software metrics
• Assess information assurance risks
500R on Information Assurance

• The process should be adaptive
• Employs the best practices known to reduce risk
• Systems shall be designed to ensure
  – Confidentiality
  – Availability
  – Integrity
  – Authentication
  – Non-repudiation
Software Acquisition Capability Maturity Model

- Developed by Carnegie Mellon, DoD, and other experts
- Defines levels similar to the software engineering capability model

<table>
<thead>
<tr>
<th>Level</th>
<th>Focus</th>
<th>Key Process Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-Initial</td>
<td>Competent people and heroics</td>
<td>N/A</td>
</tr>
<tr>
<td>2-Repeatable</td>
<td>Basic Project</td>
<td>Evaluation, Project Management</td>
</tr>
<tr>
<td>Management</td>
<td></td>
<td>Req. Development and management, Soft. Acquisition planning</td>
</tr>
</tbody>
</table>

# SA-CMM Levels

<table>
<thead>
<tr>
<th>Level</th>
<th>Focus</th>
<th>Key Process Areas</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-Defined</td>
<td>Process Standardization</td>
<td>Training program</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Acquisition risk management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Contract performance management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>User requirements</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Process definition and maintenance</td>
</tr>
<tr>
<td>4-Quantitative</td>
<td>Quantitative Management</td>
<td>Quantitative acquisition management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Quantitative process management</td>
</tr>
<tr>
<td>5-Optimizing</td>
<td>Continuous process improvement</td>
<td>Acquisition innovation management</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Continuous process improvement</td>
</tr>
</tbody>
</table>
Office of the Secretary of Defense Acquisition Reform

• Published by OSD in 1994 to streamline acquisition management

• Lists 10 principles
  – “Empower People to Manage-Not Avoid Risks”
    • Give incentives to those who take the first step
    • Encourage innovative work strategies
Office of the Secretary of Defense Acquisition Reform

– “Operate in Integrated Product Teams”
  • Replace functional design approach with teams
  • Resolve issues at lowest possible management level
  • Partner and team with industry

– “Reduce Cycle Time by 50 Percent”
  • Organize to reduce number of hands on project
  • Make cost performance trade-offs early in the process
OSD Acquisition Reform Principles

– “Expand Use of Commercial Products and Processes”
  • Research global commercial market before commitment
  • Begin and maintain dialogue with industry

– “Use Performance Specifications and Non-government Standards”
  • Minimize gov’t unique terms and conditions
  • Use performance specifications as the preferred choice
OSD Acquisition Reform Principles

– “Issue Solicitations That Reflect the Quality of a World Class Buyer”
  • Write statements that specify “what”, not “how”
  • Emphasize electronic commerce
  • Coordinate in advance to gain mutual understanding of requirements

– “Procure Goods and Services with ‘Best Value’ Techniques”
  • Evaluate bids on a ‘total-cost-of-ownership’ to seek out qualities other than lowest price
  • Use past performance metrics
  • Debrief clients promptly to avoid confusion and protest
OSD Acquisition Reform Principles

– “Test and Inspect in the Least Obtrusive Manner to Add Value to the Process or Product”
  • Make testers/evaluators value-added assets from the start
  • Take advantage of contract testing
  • Use modeling and simulation to reduce time

– “Manage Contracts from End Results”
  • Focus on the customer and the product or service required
  • Control performance specifications and let customer design
  • Operate on basis of trust to estimate performance risk
Types of Acquisitions

• Contracts
  – Entering into a legally binding document
  – Damages that can incur

• Service level agreements
  – A specific type of contract
  – Example of SLA
    • The Third-party Service provider

• Problem Management
Contracts

• Contracts
  – Fundamentally: Agreement to do or not do something specified in terms and conditions
  – Forms
    • Written (Fully/Partially)
    • Orally

• Entering into a contract
  – Parties entering contract have mutual assent and understanding of term
  – Individuals must have capacity and ability to enter into contract
    • i.e. Minors and mentally challenged
  – Unfair or biased contracts cannot be held up legally in court
Damages from Contract

• Contract damages ensure
  – Injured party receives compensation
  – Injured party may recover an amount to compensate
    • i.e. Loss of profit

• Limitations of contract damages
  – Losses that were foreseeable
  – Losses that could have been avoided
  – Damages due to mental or emotional distress
  – Punitive damages
Contract Performance

• Payment should be made for services actually rendered
  – A defaulting party may under-perform, yet still receive payment
• Contract obligations may rely on events to occur
  – Contracts may be voided if the event has occurred or not occurred
• The performance of one party may rely on the performance of another party
  – Exception: Its performance may not be impeded
• Actual Breach – unwarranted failure to perform
• Anticipatory Breach – repudiation of a contract
Service Level Agreements

• Contract between a customer and provider
  – Guarantees mutually-agreed upon quality of service
  – Need to define metrics
    • Average CPU usage
    • Average response time
    • Turnaround time
    • Baseline vs. actual performance
    • Transaction volumes
    • Usage rates
    • Number of users
SLA for Telecommunications

• Issues address in the SLA
  – Help desk support
  – Bandwidth to be provided
  – Required guarantee up time
  – Burst bandwidth available to users
  – Quality of service for different types of service
  – Penalties paid by the provider if quality of service is not met
Third-party Service Providers

• Classic example: Internet Service Provider (ISP)

• Types of liability
  – Vicarious: Imposes legal responsibility on an individual not related to the incident
    • Ex: Respondeat Superior – supervisor is legally responsible for employee
    • Exception – Contractor intentionally harms the provider, without the client’s knowledge
  – Contributory Infringer: “one who has control over copyrighted material, but was re-released without the owner’s consent”
Problem Management

• Problem management defined as a set of
  – Policies
  – Procedures
  – Tools to manage and resolve problems

• Categories of problems for Info. Sec.
  – Unexpected Events
  – Compromise of confidentiality, integrity, and availability
  – Divergence from best practices or standards
  – Abnormal Situations
Problem Management Tools

• Aid in the problem management using project management tools
  – Incorporate standards, policies and procedures
  – Tracking problems
  – Identify individuals responsible for handling a problem
  – Display status of the problem
  – Record time required to solve problem
  – Prioritizing problem resolution assignments

• Positive and Negative views
  – Competition is positive
  – Conflict of interest is negative
Monitoring and Auditing

• Both are used by organizations to maintain operational assurance

• Monitoring vs. Auditing
  – Auditing: performed one-time or periodically
  – Monitoring: performed real-time

• Reviews can be held
  – Application Level
  – System-wide level

• Monitoring and Auditing Methods
  – Conducted in-house or external auditors
Monitoring

- Incorporates mechanisms, tools, and techniques
- Information Systems monitoring
  - Illegal software installation
  - Hardware faults and error states
  - Operational events for anomalies
- Intrusion Detection
  - Assist in detective analysis of intrusion attempts
  - Also used to create sample of traffic patterns
- Violation Analysis
  - Must establish a clipping level
    - Baseline of user activity considered normal
    - Enables a system to ignore normal user errors
  - Violation is raised when clipping level is exceeded
Monitoring Violation Analysis

• Clipping levels & profile-based IDS can track the following
  – Repetitive mistakes exceeding clipping level
  – Individuals exceeding their authority
  – Many people with unrestricted access
  – Patterns indicating intrusion attempts

• Profiles are patterns of user characteristics
  – Processing exceptions
  – Resource utilization
  – Patterns of actions performed
Auditing

- Present information to management regarding system operation
- Used to reduce and mitigate risk
  - Analysis between potential risk and cost to repair damage
- Three types of risk
  - *Control*: controls implemented will not prevent, correct, or detect on a timely basis
  - *Detection*: procedures performed by audit team will not yield a positive detection
  - *Inherent*: susceptibility of process to commit relevant errors on its own
Steps for Basic Auditing

• Gather, store, and review system logs
  – Logon and logout
  – Permission changes
  – Using privileged commands
  – Removable media
  – System startup and shutdown
  – Access controls
    • Date and time of access
    • Entrance of access (network share)
    • Whether attempt was successful
    • Who attempted access
Steps for Basic Auditing

- Review system security and identify potential breaches
  - Breach discovered – retrace events leading up to breach and activities performed during the breach
- Info. security auditing performed at network layer
  - Subnet gateways
  - Servers (email, file, app, etc.)
  - User workstation
Security Auditing

• Two types of auditors
  – Internal – Work for the organization
  – External – Certified public accountants (CPA)

• IT auditors
  – Backup controls
  – System and transaction controls
  – Data library procedures
  – Data center security
  – Contingency plans
  – Recommends
    • Improvement to controls
    • Participate in system’s development to avoid re-engineering costs
Audit Trails

• Audits trails are needed for forensic analysis
  – Able to follow the clues and reconstruct the intrusion

• Audits logs should contain the following
  – The transaction date and time
  – Which user processed transaction
  – Terminal that was used

• The following audit logs should also be checked
  – Amendments to production jobs
  – Production job reruns
  – Computer operator practices

• Electronic form should be saved
Problem Management and Auditing

• To reduce failures to a manageable level
• To prevent the occurrence or reoccurrence of a problem
• To mitigate the negative effect of problems on computing services and resources
Break Time
Overview

• Configuration Management
• Security Review and Testing
• Security Awareness and Education
• Operational Security
Configuration Management

• Procedures for System Changes
  – Configuration Identification
  – Configuration Control
  – Configuration Status Accounting
  – Configuration Auditing
  – Documentation Change Control

• Patches
Configuration Management

- Configuration Management is the process of tracking and approving changes to a system.
- The goals of defining and enforcing Configuration Management procedures are:
  - To make sure that the security of a system is not compromised by a change.
  - Allow for system rollback.
  - Keep documentation up to date to minimize impact on other systems.
  - Ensure change is orderly and user base is informed.
Procedures for System Changes

• The general procedure for implementing a system change is as follows:
  – Apply for approval
  – Catalog the intended change
  – Schedule the change
  – Implement the change
  – Report the change to all appropriate parties
Configuration Identification

• This is the process of breaking down a system into smaller, more manageable parts
• This helps by making changes easier to track and understand
• The smaller pieces are called Configuration Items (CIs)
• Definition - A CI is a uniquely identifiable subset of the system that represents the smallest portion to be subject to independent configuration control procedures
Configuration Control

• Goal: To ensure that changes get approved before they are implemented and that implemented changes are complete and accurate

• Configuration Control Board (CCB) – Group of personnel who centrally:
  – Coordinate analytical tasks
  – Approve system changes
  – Review the change implementation
  – Supervise documentation
Configuration Status Accounting

• Goal: To document the configuration control activities and anything else needed to manage a system configuration

• If this accounting is done correctly it can help find flaws or inefficiency in the configuration control process
Configuration Auditing

• This step is to ensure quality assurance
• All of the accounting must be periodically checked against actual progress
• There should also be checks to ensure compliance with management policies
• This step is often carried out by a review team
Documentation Change Control

• Keeping and updating detailed documentation on the system and its changes is crucial
• It is important to identify and keep track of all aspects of a system. Some things that should be documented:
  – Changes to the system infrastructure
  – Changes to security policies or procedures
  – Changes to disaster recovery or business continuity plans
  – Facility environment changes
Patches

• One of the most common system changes is patching software that is in use
• Believe it or not you don’t always patch!
• For instance if it will cost $10,000 to patch all your computers but the potential damage is only $7,000 you would not patch
• This is an extremely important issue that is often overlooked
Patching Considerations

• Formula for patching cost:
  Cost to Patch = (Hours x Rate x Systems) +
  (Patch Failure% x (Hours x Rate x Systems))

• There are factors other than cost that should be considered (e.g. Security, likelihood of exploit)

• All patches should be reviewed and tested before and after implementation to assure that the security of the system is not negatively effected

• Keep in mind that the risks involved in not patching a system change as time goes on
More on Patching Costs

• The ideal time to patch is as soon as the cost to patch is less than or equal to the cost not to patch

• Patching costs include:
  – Man hours to patch
  – Man hours to correct failed patches
  – Note: Can be reduced by automated patching systems
  – Possibly man hours to create patch

• Costs for not patching include:
  – Lost productivity (both end user and IT personnel)
  – Loss of revenue
  – Legal costs
  – Intellectual property losses
  – Loss of stored assets
Security Review and Testing

• Reasons for Testing
• Types of Testing
• Scanning Methods (High level overview)
• Testing Issues
Reasons for Testing

• There is only one way to tell if your system is as secure as you want it and that’s testing

• Internal and external testing can reveal security holes that the system creators missed (either due to faulty design or implementation)

• Reviews and testing can reveal flaws in not only the system hardware and software but also policies, documentation, and audit capabilities
Types of Testing

• Internal Testing – done with access to system internals (e.g. building access, user account access)

• External Testing – done from outside of the system (e.g. like an attacker)

• System Scanning – process of collecting information about a device or network
Goals of Network Attack Testing
(aka Penetration Testing)

• Network reconnaissance – Find out valuable information about a network through scanning
• Gaining system access – This is one of the goals of testing. In a perfect system this should not be attainable
• Removing evidence of the attack – There should be some system aspect that prevents this
Scanning Methods

• Vulnerability Scanning
  – Discovery Scanning
  – Workstation Scanning
  – Server Scanning

• Scanning tools (in case you’re interested)
  – NMap
  – Tcpview
  – Hping
  – Nessus
Testing Issues

• From a management perspective:
  – Tests should be thorough and complete
  – Testing can cause strains on the system (e.g. heavy traffic and system failures) and should be conducted after hours
  – After hours testing may be inaccurate due to non-normal system usage

• From a technical perspective
  – Careful analysis of results must be conducted in order to identify false positives and maybe even false negatives
Security Awareness and Education

- Reasons for Education
- Methods of Educating
- Integrating Awareness
Reasons for Education

• A system is no more secure than its weakest link and often people are that link
• An uneducated staff is an insecure staff
• The goals of security education are:
  – To make users aware of their security responsibilities and teach them best practices to mold their behavior
  – Develop the users skills and knowledge so that they can perform their jobs more securely
  – Train in order to operate security programs for organizations and systems
NIST Recommendations

• When setting up a computer security awareness or education program keep the following in mind:
  – Identify program scope, goals, and objectives
  – Identify training staff
  – Identify target audiences
  – Motivate management and employees
  – Administer the program
  – Maintain the program
  – Evaluate the program
Integrating Awareness

• It is important to make security awareness an ongoing process
• This is because people forget or become lax in their attention to security; also new employees need to be trained as well
• Some methods of integrating awareness are:
  – Live interactive presentations
  – Distribution of publications
  – Incentives
  – Reminders
Benefits of Security Awareness

• Obviously a more secure system. This is done by increasing the effectiveness of protection controls

• Reduce unauthorized actions attempted by personnel

• Help avoid fraud, waste, and abuse of computing resources
Operational Security

• What is OPSEC
• Why is it Important
• What can be Done
What is OPSEC

• OPSEC stands for Operations Security
• It is pretty much the same thing as external and internal penetration testing
• The difference is that it also includes security awareness and education techniques
• This allows for the lessons learned in penetration testing to be shared with the entire staff
• Also the data obtained is in some cases less obvious than traditional penetration testing
Why is it Important

• Yes we spoke about most of this already but it’s really important so here are some things we didn’t mention

• Here are some subtle ways that data can be leaked:
  – Dates, times and places
  – Website information like project summaries
  – Documentation including information acronyms, contingency plans, or funding
What can be Done

• Analyze what information is available to adversaries and how valuable it is
• Determine how probable it is that an adversary will gain this information
• Develop a set of operational practices that make it harder for an adversary to obtain the more important information
References

• The CISM Prep Guide, Chapter 4
• “Operations Security (OPSEC): The Basics”,
  http://www.nswc.navy.mil/ISSEC/Docs/Ref/GenerallInfo/opsec_basics.html#indicators
• “Generally Accepted Principles and Practices for Securing Information Technology Systems”,
  NIST Special Publication 800-14
• “National Training Standard for System Administration in Information Systems Security”,
  NIST Publication 4013
• Information Security Magazine, February 2004,
  “A Patch in Time” by Pete Lindstrom