Risk Analysis:
A Practical Approach

The Eighth National

HIPAA Summit

Monday, March 8, 2004

Tom Walsh, CISSP

Tom Walsh Consulting, LLC

Tom Walsh Consulting, LLC ◆ Overland Park, KS ◆ www.tomwalshconsulting.com

Phone: 913-696-1573 ◆ e-mail: twalshconsulting@aol.com

Session Objectives

- Describe the steps involved in a risk assessment and analysis
- Discuss the creation of risk profiles
- Review the most common mistakes made when conducting a risk analysis

Based upon NIST Special Publications:
800-30 *Risk Management Guide for Information Technology Systems*
800-26 *Security Self-Assessment Guide for Information Technology Systems*

Risk Assessment / Analysis

Under HIPAA each covered entity:

- Assess its own security risks
- Determines its risk tolerance or risk aversion
- Devises, implements, and maintains appropriate security to address its business requirements
- Documents its security decisions

Does not imply that organizations are given complete discretion to make their own rules.

Terminology

Threat – Potential danger to a computer, network, or data

Vulnerability – An inherent weakness or absence of a safeguard that could be exploited by a threat

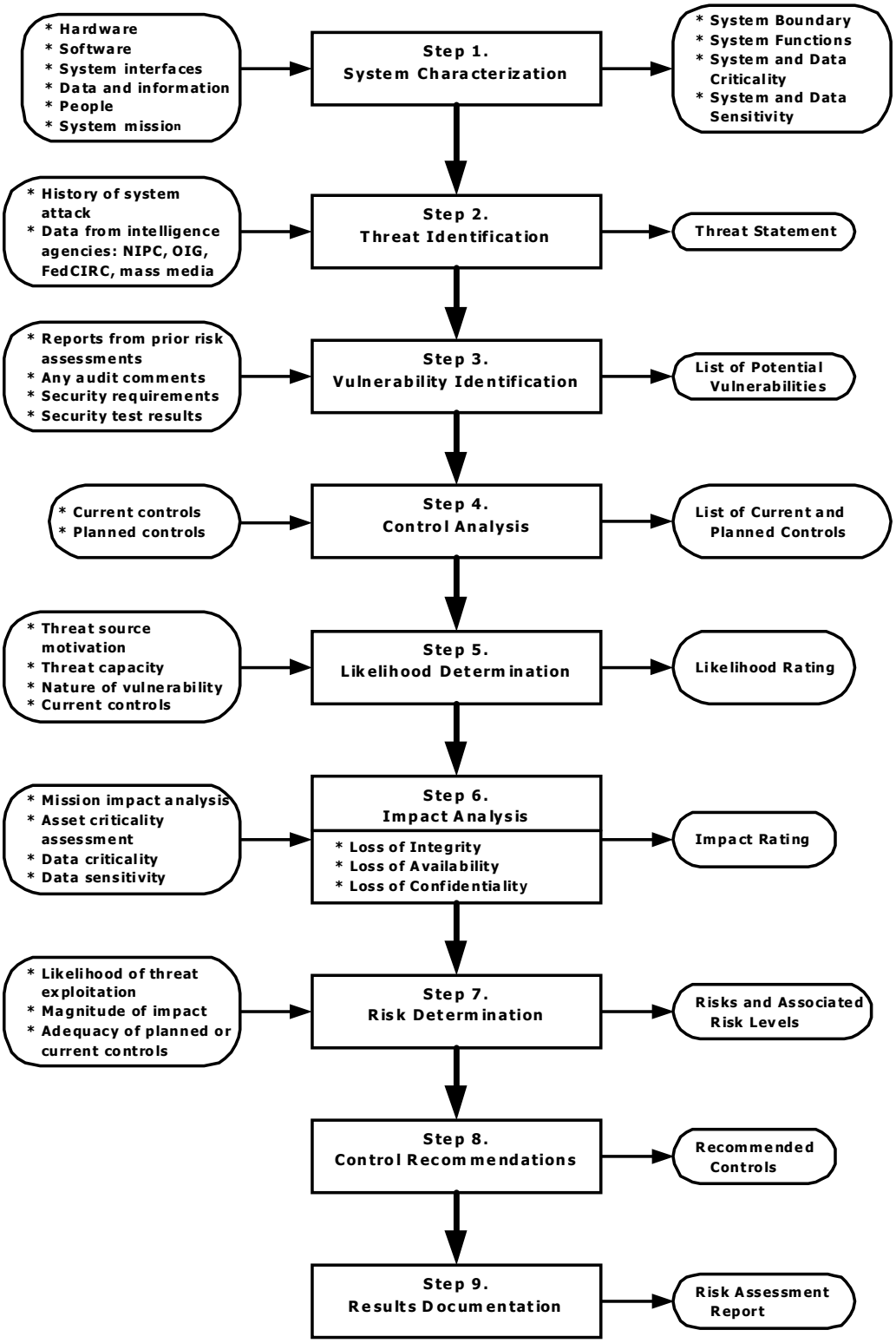
Risk – Probability of a threat exploiting a vulnerability and exposing an asset to a loss

Countermeasure, safeguard, or controls – Mitigates and reduces potential risks

General Support System is an interconnected information resource under the same direct management control that shares common functionality. It normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications. Individual applications support different mission-related functions. Users may be from the same or different organizations.
(Source: NIST SP 800-26 *Security Self-Assessment Guide for Information Technology Systems*)

Major Application is an application that requires special attention to security due to the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to, or modification of, the information in the application. A breach in a major application might comprise many individual application programs and hardware, software, and telecommunications components. Major applications can be either a major software application or a combination of hardware/software where the only purpose of the system is to support a specific mission-related function.
(Source: NIST SP 800-26 *Security Self-Assessment Guide for Information Technology Systems*)

Risk assessment and analysis is like predicting the weather.



1. System Characterization

- Hardware
  - Servers
  - Mainframes
  - Network equipment (includes wireless)
  - Mobile computing devices (Laptops, PDA's, etc.)
  - Biomedical equipment
- Software
  - Operating systems
  - Applications and programs
- Information and/or Data
  - Highly sensitive, confidential or mission critical

2. Threat Identification

List all possible threats but focus on the most probable threats.

- Acts of Nature
  - Some type of natural disaster that is beyond our control
- Acts of Man
  - Unintentional or accidental
  - Intentional
- Environmental
  - Power outage, broken water pipe, network outage, cut LAN cable

3. Vulnerability Identification

- Hardware
  - BIOS (Basic Input / Output Instructions)
- Software
  - Operating Systems
  - Applications
- Environmental
  - Lack of environmental controls
  - Lack of physical safeguards
- Operational practices
  - Lack of policies and procedures
  - Untrained personnel

- **After identifying the threats and vulnerabilities, determine risks considering existing controls**

  Risk = Threat x Vulnerability x Impact

  If any one of the three equals zero, there is no risk

- **Risks are rated by the likelihood of a threat exploiting a vulnerability and the possible consequences or impact**

4. Control Analysis

Manual data collection involves developing questionnaires and conducting interviews and surveys with the organization's staff.

- Survey or checklists are usually used to collect data on existing controls

  Most common mistake – Trying to ask too many questions

Access Control -	Yes	No	N/A
18. Is there an access control list of authorized users?			
19. Are users only granted access by a request from management?			
20. Are users' default privileges set for least privilege?			
21. Are user accounts locked out after five unsuccessful log-in attempts?			
22. Is there a method in place to notify the server administrator when a user's access is no longer required (i.e. user termination or transfer)?			

5. Likelihood

(Source: NIST SP 800-30 Risk Management Guide for Information Technology Systems)

Likelihood Level	Likelihood Definition
High	The threat-source is highly motivated and sufficiently capable, and controls to prevent the vulnerability from being exercised are ineffective.
Medium	The threat-source is motivated and capable, but controls are in place that may impede successful exercise of the vulnerability.
Low	The threat-source lacks motivation or capability, or controls are in place to prevent, or at least significantly impede, the vulnerability from being exercised.

6. Impact Analysis

Magnitude of Impact	Impact Definition
High	Exercise of the vulnerability (1) may result in the high costly loss of major tangible assets or resources; (2) may significantly violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human death or serious injury.
Medium	Exercise of the vulnerability (1) may result in the costly loss of tangible assets or resources; (2) may violate, harm, or impede an organization's mission, reputation, or interest; or (3) may result in human injury.
Low	Exercise of the vulnerability (1) may result in the loss of some tangible assets or resources or (2) may noticeably affect an organization's mission, reputation, or interest.

7. Risk Determination

Determining a "Risk Score"

The higher the number, the greater your risks.

Source: The OCTAVE℠ Approach

Impact	L	M	H
H	3	6	9
M	2	4	6
L	1	2	3

Probability of Occurrence

8. Control Recommendations

Types of Controls

- Technical
- Non-technical

Purpose of Controls

- Prevention
- Detection
- Assurance
- Recovery

- Technical (tools)
  - Freeware
  - Existing security features not in use
  - Purchase software and/or hardware
- Non-technical
  - Policies, procedures, plans, etc.
  - Practices
  - Training (Practices and behavior)

9. Results Documentation

- Overview
  - This report summarizes the residual risks inherent in the [system name] based upon the assessment and analysis conducted _____.
- System description
- Description of Risk Analysis Approach
- Results (Findings)
- Recommendations
- Information/Data Owner Comments
- Statement of Understanding
  "I, the Information/Data Owner, understand that the threats, identified in this risk analysis, could cause a negative impact to business operations supported by this information system. I have been informed of the risks for operation of the system in its current configuration."

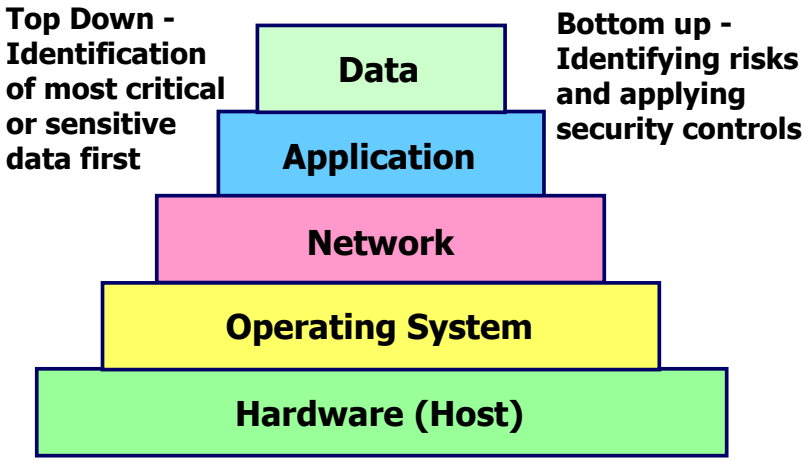
Creating Risk Profiles

- Grouping information assets and/or systems into categories
- Determining most common threats and vulnerabilities
- Reviewing the existing safeguards and controls
- Determining shared or common risks
- Finding the most cost-effective safeguards and controls for risks

Things to Note:

- Threats may vary from general profiles based upon geographical location.
- Vulnerabilities are based upon adequacy of current security controls and the maturity of the information security program.
- Threats are always changing and the profiles need to be updated periodically and modified as the environment changes.
- Updating profiles can be an efficient way to manage risks

Recommendation: Use your Information Security Incident Reporting system to help define threats and probabilities.



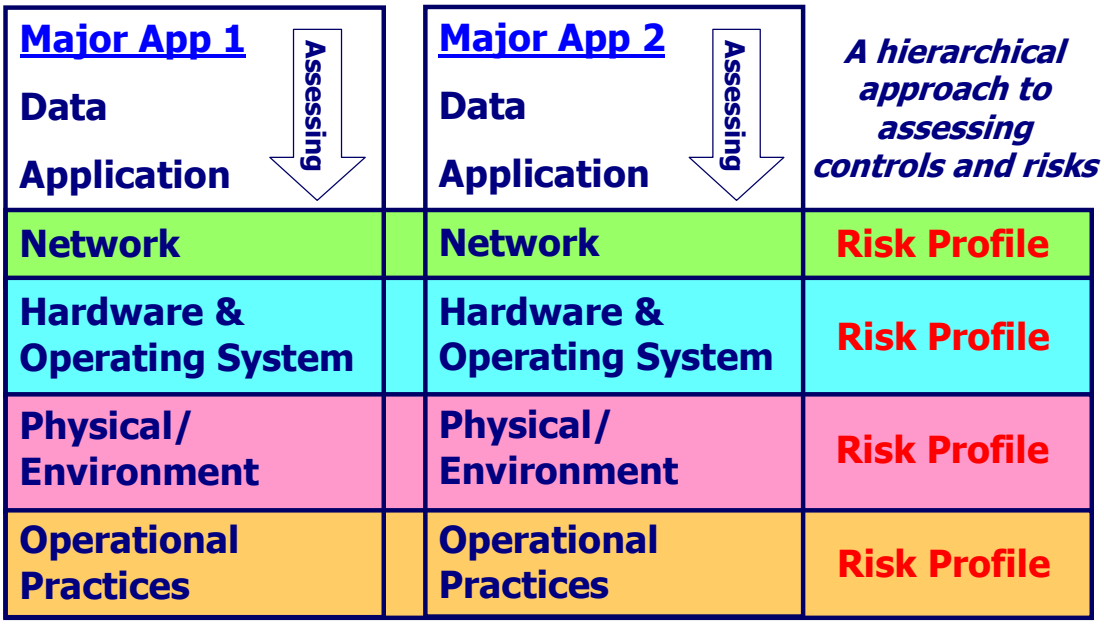
Data Collection

"Manual data collection involves developing questionnaires and conducting interviews and surveys with the organization's staff. More useful data becomes available from semi automated and automated data sources, such as self-assessment tools, certification and accreditation (C&A) databases, incident reporting and response databases, and other data sources as a security program matures. Metrics data collection is fully automated when all data is gathered by using automated data sources without human involvement or intervention." ***Source:*** *NIST SP 800-30*

Risk Analysis Documentation

Threats	Vulnerability	Impact or Loss	Prob. Score	Impact Score	Risk Score
Hardware or mechanical failure	No backup system; No redundancy system	Business interruption (Availability or Integrity)	H	H	9
Workforce Behavior - Careless act of employees; Accidental loss or disclosure of PHI	Lack of training; Lack of adequate access controls; No security incident handling procedures; Inadequate sanctions; No media re-use policy; No data destruction procedures	Confidentiality, Integrity, or Availability Litigation: Criminal or civil	H	M	6
Environmental (fire, water damage, heat, etc.)	Insufficient disaster or contingency planning	Business interruption (Availability)	L	H	3

Risk Profile Approach



Good security now is better than perfect security never.

Finding the "Right" Security Control

- Studies conducted by research firms
- Buyer's guide from information security trade journals
- Professional organizations
- Referrals from other organizations

Common Mistakes

- Trying to mitigate every possible risk
- Risk can either be:
  - Mitigated/Reduced (Applying controls)
  - Transferred (Insuring against a loss)
  - Accepted (Doing nothing, but recognizing risk)
- Risk should be handled in a cost-effective manner relative to the value of the asset

Common Mistakes

- Considering a “gap analysis” a risk analysis
- Purchasing a risk analysis tool without a clearly defined process
- Conducting a quantitative analysis
- Failing to understand the objectives of a risk analysis
  - Prioritized task list for safeguards and controls based upon risk

Common Mistakes

- Focusing on the trivial many instead of the critical few
- Failing to set borders for the risk analysis:
  - Analyzing all information systems
  - Analyzing all systems that process and store ePHI
- Failing to maintain information security incident reporting procedures

Keeping it Manageable

- Scope the assessment
  - Focus on the most critical and sensitive information systems
- Get Information/Data Owners involved
  - They need to determine how risks will be managed
- Manage expectations
  - Each year the risk picture will become clearer

Conclusion

"… the risk management process should not be treated primarily as a technical function carried out by the IT experts who operate and manage the IT system, but as an essential management function of the organization."

NIST Special Publications 800-30 Risk Management Guide for Information Technology Systems

Resources and References

- NIST Special Publication 800 series: http://csrc.nist.gov/publications/nistpubs/index.html
- CERT/CC at Carnegie Mellon University (www.cert.org/stats/cert_stats.html)
- Peltier, Thomas R. *Information Security Risk Analysis*. New York: Auerbach Publications, 2001
- Project COAST (Computer Operations, Audit and Security Technology), Purdue University, www.cerias.purdue.edu/coast – OCTAVE (Operational Critical Threat, Asset, and Vulnerability Evaluation)
- CSI / FBI Computer Crime and Security Survey (annual survey results) (http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2003.pdf)
- SecurityStats.com (http://www.secstats.com/about.asp)
- Alberts, Christopher, and Audrey Dorofee. *Managing Information Security Risks, The OCTAVE Method*. Boston: Pearson Education, 2003.
- ISO 17799:2000, Code of Practice for Information Security Management
- "Best Practices for Compliance with the Final Security Rule" by Tom Walsh, published by HIMSS in the Journal of Healthcare Information Management, Volume 17, Number 3, Summer 2003

A successful risk management program will rely on:

(1) Senior management's commitment;

(2) The full support and participation of the IT team;

(3) The competence of the risk assessment team, which must have the expertise to apply the risk assessment methodology to a specific site and system, identify mission risks, and provide cost-effective safeguards that meet the needs of the organization;

(4) The awareness and cooperation of members of the user community who must follow procedures and comply with the implemented controls to safeguard the mission of their organization; and

(5) An ongoing evaluation and assessment of the IT-related mission risks.

(Source: NIST SP 800-30 Risk Management Guide for Information Technology Systems)

