Risk Analysis Webinar

Tom Walsh, CISSP

tw-Security

Overland Park, KS

tw Security
Healthcare Information Security

Webinar Objectives

- Explain the difference between a risk analysis and risk assessment
- Review the HIPAA requirements for risk analysis
- Explain key components of a risk analysis
- Explain key security risks
- Discuss Meaningful Use and what is required to attest for the core objective of risk analysis
- Describe risk analysis is a journey, not an end (managing risks)

Introduction – Tom Walsh

- **Certified Information Systems Security Professional (CISSP)**
- **Founder and Managing Partner of tw-Security**
  (formerly: Tom Walsh Consulting, LLC - In business for 14+ years)
- **Co-authored four books on healthcare security**
  – Published by AMA, AHIMA, and HIMSS *(two books)*
- **Former information security manager for large healthcare system in Kansas City metro area**
- **Started working in information security in 1992**
- **A little nerdy, but overall, a nice guy ☺**

Assessment versus Analysis

Assessment

A **judgment** about something based on an **understanding** of the situation

Analysis

The **close examination** of something **in detail** in order to draw **conclusions** from it

Requirements

Why a risk analysis is necessary

HIPAA – Risk Analysis

§ 164.308(a)(1)(ii)(A) Risk analysis *(Required)*

Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity [or business associate].

A risk analysis is <u>not</u> an evaluation of compliance with the HIPAA Security Rule!

ONC's SRA Tool

- **Security Risk Assessment (SRA) Tool**
  - Created by the Office of the National Coordinator
- **When printed, the SRA Tool = 436 pages**
- **ONC estimates that it will only take 6 hours to complete the 436 pages of the SRA tool**
- **The tool is for evaluating compliance gaps with HIPAA – it is not a true risk analysis**
- **There is a lot of critical security topics missing from the tool**

Meaningful Use – Stage 1

Objective:

Ensure adequate privacy and security protections for personal health information

Measure:

Conduct or review a security risk analysis in accordance per 45 CFR 164.308 (a)(1) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.

Meaningful Use – Stage 2

Objective:

Protect electronic health information created or maintained by the Certified EHR Technology through the implementation of appropriate technical capabilities

Measure:

Conduct or review a security risk analysis in accordance with the requirements under 45 CFR 164.308(a)(1), including addressing the encryption/security of data at rest in accordance with requirements under 45 CFR 164.312 (a)(2)(iv) and 45 CFR 164.306(d)(3), and implement security updates as necessary and correct identified security deficiencies as part of the EP's risk management process.

PCI DSS Requirement 12.2
(Payment Card Industry Data Security Standard)

12.2 Implement a risk-assessment process that:

- Is performed at least annually and upon significant changes to the environment (for example, acquisition, merger, relocation, etc.),

A risk assessment enables an organization to identify threats and associated vulnerabilities with the potential to negatively impact their business. Resources can then be effectively allocated to implement controls that reduce the likelihood and/or the potential impact of the threat being realized.

Key words:

"…performed at least annually and upon significant changes…"

Threats, controls, vulnerabilities, likelihood, and impact

Risk Analysis

Each organization has to:

- **Assess its own security risks**
- **Determine its risk tolerance or risk aversion**
- **Devise, implement, and maintain appropriate security to address its business requirements**
- **Document its security decisions**

Risk Analysis – A systematic and ongoing process of identifying threats, controls, vulnerabilities, likelihood, impact, and an overall rating of risk.

Risk Analysis Steps

Reprinted with permission from: Susan Lucci and Tom Walsh Consulting, LLC

Risk Analysis

The nine steps in the risk analysis process:

1. System characterization
2. Threat identification
3. Control assessment
4. Vulnerability identification
5. Likelihood determination
6. Impact analysis
7. Risk determination
8. Control recommendations
9. Results documentation

Based upon the original National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30, *Risk Management Guide for Information Technology Systems*

1. System Characterization

- **Create an inventory of applications and systems**
  - Major applications
  - General support systems
    - Computer workstations
    - Laptops
    - Smartphones and tablets
    - Network (LAN, wireless, extranet, etc.)
    - Data Center or Server Room

Threats are based upon information asset types.

2. Threat Identification

- **Identify reasonably anticipated threats**
  - Acts of nature
    - Natural disaster that is beyond our control
    - Threats affecting the organization as a whole
  - Acts of man
    - Unintentional or accidental
    - Intentional
  - Environmental threats
    - Generally, threats affecting Data Center or Server Room operations

Unreasonable Threats

- Chemical spills
- Biological contamination
- Nuclear mishaps
- Aircraft accident
- Civil unrest / Rioting
- Bomb threats
- Sinking ground
- Tsunami
- Volcano eruption
- Blackmail
- Substance abuse
- Inflation

Thorough does not mean unreasonable.

3. Control Assessment

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

Checklists are usually used to assess existing controls.

4. Vulnerability Identification

- **Hardware**
  - Improperly configured equipment
- **Software**
  - Operating systems needing patching
  - Poorly written applications
- **Environmental**
  - Lack of environmental controls
  - Lack of physical safeguards
- **Operational practices**
  - Lack of policies and procedures
  - Untrained personnel

Checklist – SAMPLE

Authentication		Yes	No	D/K	N/A
17	Are users forced to change their password from the initially assigned password at first login?				
18	Indicate the minimum number of characters for passwords: _____				
19	Is password complexity enforced?				
	If yes, indicate the enforced complexity rules *(For example, includes a number, upper/lower case, etc.)*: _____ _____ _____				
20	Is password expiration forced by the application?				
	If yes, indicate the frequency of change: _____				
21	Are rules enforced to prevent password reuse?				
	If yes, specify the history, the number of times a different password has to be selected before a user can reuse a previous passwords: _____				

"Yes" = Control; "No" = Vulnerability

5. Likelihood Determination

What is the likelihood or probability of each threat circumventing the existing controls?

- **Likelihood can be rated as being:**
  - High, Medium, or Low
- **To maintain consistency your organization should include some definitions of those ratings**

6. Impact Determination

Evaluate what that would do to your organization if a threat was realized.

- **Impact can be rated as being**
  - High, Medium, or Low
- **To maintain consistency, your organization should include some definitions of those ratings**

It can be difficult to precisely quantify the impacts if a threat was realized.

6. Impact – Possible Consequences

- **Confidentiality**
- **Integrity**
- **Availability**

- **Opportunity (financial)**
- **Reputation**
- **Litigation**

7. Risk Determination

"Risk is a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of:

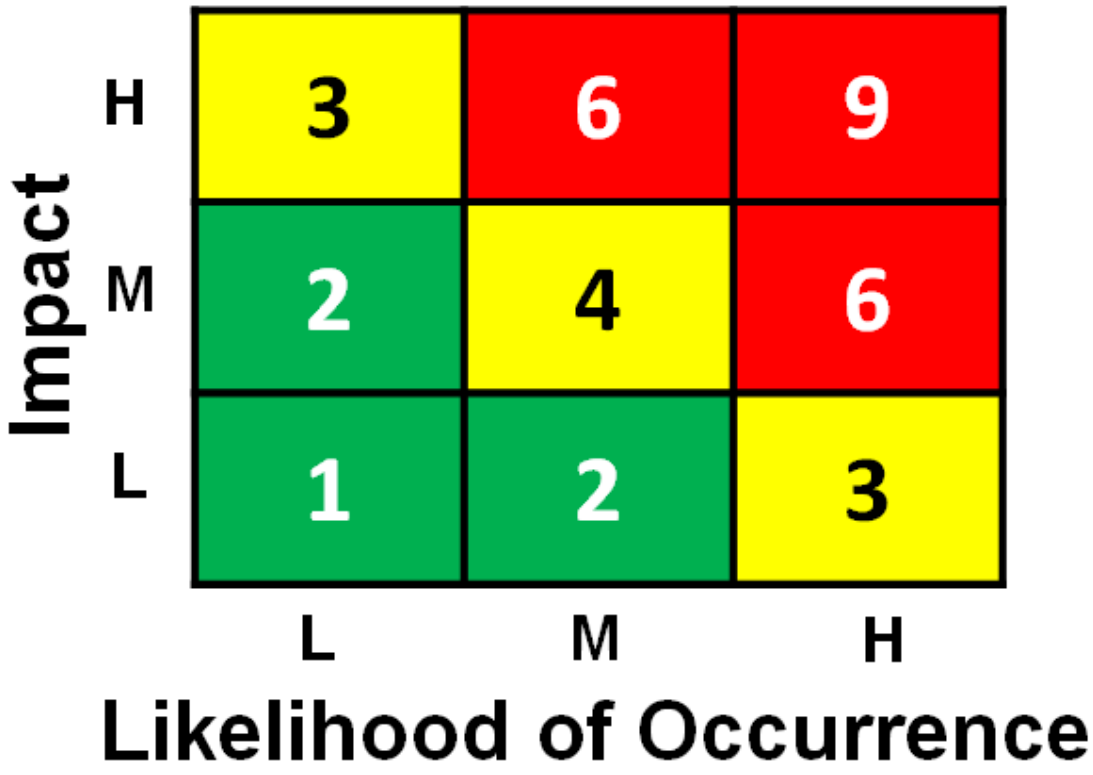
(i) the adverse impacts that would arise if the circumstance or event occurs; and

(ii) the likelihood of occurrence."

Source: National Institute of Standards and Technology (NIST) Special Publication (SP) 800-30 *Guide for Conducting Risk Assessments*

7. Risk Determination

The OCTAVE approach to calculate a risk score:



Risk Score – SAMPLE

Impact	Likelihood (Probability)			
	Very High (4)	**High (3)**	**Medium (2)**	**Low (1)**
Very High Impact (16)	Very High (64)	Very High (48)	High (32)	High (16)
High Impact (8)	High (32)	High (24)	High (16)	Medium (8)
Medium Impact (4)	High (16)	Medium (12)	Medium (8)	Low (4)
Low Impact (2)	Medium (8)	Low (6)	Low (4)	Low (2)

Source: AHIMA Practice Brief, *Security Risk Analysis and Management: An Overview*

8. Recommended Controls

- **Provide recommendations to address each vulnerability (if possible) to reduce or manage risks appropriately**

Vulnerability	Control Recommendation
Audit logs are not regularly reviewed and are primarily used for problem solving	Create procedures to randomly audit users; formalize log review responsibilities and procedures
User's account is not disabled after a predetermined number of unsuccessful logon attempts	Consider locking out a user's account after five consecutive unsuccessful logon attempts
Disaster recovery plan has not been created; a formal business impact analysis has not been conducted	Conduct a formal business impact analysis (BIA); create a disaster recovery plan that outlines a systematic approach to recovery based upon the needs of the business as documented in a BIA

9. Results Documentation

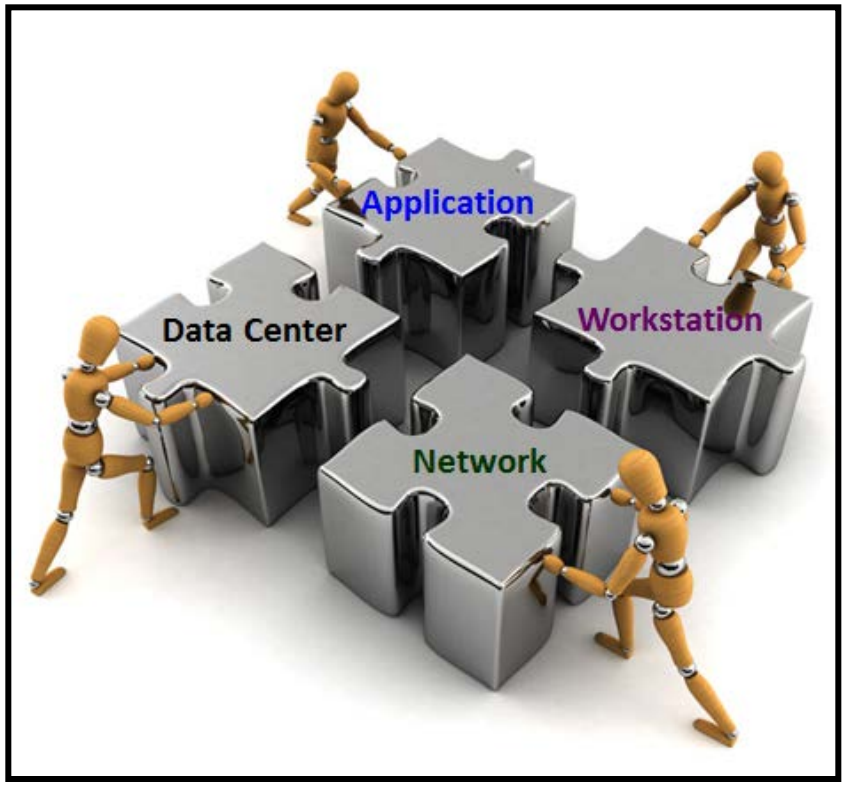
- **Create a summary of key findings, recommendations and estimates to implement**
- **Document management's decisions:**
  - Avoid the risk (Many times – not an option)
  - Mitigated/Reduced (Applying controls)
  - Transferred/Shared (Insuring against a loss) or
  - Accepted (Doing nothing, but recognizing risk)
- **Risk should be handled in a cost-effective manner relative to the value of the asset**

Key Security Risks

Key Security Risks

- **Malicious code** (phishing and ransomware)
- **Hacking or tampering by an external person**
- **Unsecured mobile devices** (smartphones and tablets)
- **Authorized user misusing their privileges** (snooping)
- **Unauthorized user or inappropriate access** (Internal)
- **System failures – no disaster recovery strategy**
- **Noncompliance with standards and regulations** (HIPAA and Payment Card Industry Data Security Standard (PCI DSS))

Risk Analysis and Meaningful Use Audits



Risk Analysis Report

Topics to address in a report:

- Overview
  (Report date, Information/Data Owner, author of report)
- Scope (Application(s) and General Support System(s)
  (Business functions, data sensitivity, criticality of system)
- Description of risk analysis approach
- Risk analysis team members
- Findings (Vulnerabilities unacceptable risks)
- Recommendations
- Information/System owner comments
- Statement of understanding – risk acceptance

Remediation Plan – SAMPLE

SAMPLE Action Plan for ABC *(ABC = Name of the application or system)*

Based on the Risk Analysis Report approved by:_____ **Date:**_____

Suggested Controls	Estimated Resources [Time (duration) and Costs (investment)]	Action Plan			Comments
		Assigned to:	Start date	Finish date	
Upgrade application ABC to version 4.3 which automatically encrypts the SSN field and other sensitive database fields	Moderate costs to implement upgrade Moderate level of effort to test and implement	**Bill Garcia** and the ABC application team	**7/20**	**9/30**	
Determine how Excel spreadsheets containing PHI will be appropriately secured	Low level of effort	**Al White** (approval)	**7/22**	**7/22**	
Consider locking out a user's account after five consecutive unsuccessful logon attempts	Low level of effort to review, approve, and implement lockout	**Susan Jackson** Practice Manager	**7/27**		
Consider creating a formal review process for disabling user accounts that have been inactive for long periods of time such as 30 – 60 days	Low to moderate level of effort to create and implement a process	**Bill Garcia** and the HIPAA Security Officer	**8/19**		Meeting scheduled for 8/19
Create procedures to randomly audit users; formalize log review responsibilities and procedures	Moderate level of effort	**HIPAA Security Officer**	**8/10**		Need to assign responsibility for audit log review
Implement the standard warning banner that notifies users of auditing and monitoring activities	Low level of effort	**Bill Garcia** and the ABC application team	**7/20**	**7/20**	IT will provide the banner wording

Meaningful Use Audits

Core Objective - Protect Electronic Health Information *(Eligible Professionals)*

"Proof that a security risk analysis of the certified EHR technology was performed prior to the end of the reporting period (i.e. report which documents the procedures performed during the analysis and the results of the analysis). If deficiencies are identified in this analysis, please supply the implementation plan; this plan should include the completion dates."

Risk Analysis – It's a Journey

Risk Analysis

- **Not a "one and done"**
- **Risk profiles are a snapshot in time – things change**
- **New vulnerabilities are being discovered**
- **A refresh of the risk analysis can be accomplished quickly**
  - What changed from the last risk analysis?

Frequency of Risk Analysis

According to Centers for Medicare & Medicaid Services (CMS) ,

"…risk assessments must be completed **at least every three years** or **whenever there is a significant change** in the environment, including, but not limited to:

- Introduction of new systems;
- Significant upgrades to existing systems;
- Retirement or disposal of systems;
- Physical relocation of IT assets;
- Introduction of new lines of business; and,
- Reorganization of the CE's [covered entity's] management or business structure."

Source: HIPAA Compliance Review Analysis and Summary of Results, released by the Centers for Medicare & Medicaid Services (CMS), in June of 2009

OCR Phase 2 – Desk Audits

- **Breach Notification Rule (BNR)** only 2 of 19 criteria
  - BNR12 Timeliness of Notification
  - BNR13 Content of Notification
- **Privacy (P)** only 3 of 89 criteria
  - P55 Notice of Privacy Practices - Content requirements
  - P58 Provision of Notice - Electronic Notice
  - P65 Right to access
- **Security (S)** only 2 of 70 criteria
  - S2 Security Management Process - Risk Analysis
  - S3 Security Management Process - Risk Management

The letters and numbers associated with the desk audit align with the numbering in OCR's *HIPAA Audit Program Protocol*

Conclusion

Risk

Likelihood **Impact**

References

- NIST Computer Security Resource Center, SP 800-30 *Guide for Conducting Risk Assessments*:
  - http://csrc.nist.gov/publications/PubsSPs.html
- *PCI DSS Risk Assessment Guidelines*:
  - https://www.pcisecuritystandards.org/documents/PCI_DSS_Risk_Assmt_Guidelines_v2.pdf
- *Operationally Critical Threat, Asset, and Vulnerability Evaluation* (OCTAVE):
  - http://www.cert.org/octave/
- International Organization of Standardization (ISO):
  - http://www.iso.org/iso/catalogue_detail?csnumber=56742

Tom Walsh, CISSP

tw-Security

Overland Park, KS

www.tw-Security.com

tom.walsh@tw-Security.com

913-696-1573

tw-Security, a nationally recognized healthcare IT security consulting firm is dedicated to helping healthcare organizations protect their information resources with hands-on experience in creating and managing information security programs.