Security Risk Analysis: What is Required and How Do You Get it Done?

§ 164.306 Security standards: General rules.

(a) *General requirements.* Covered entities and business associates must do the following:

(1) Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits.

(2) Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.

(3) Protect against any reasonably anticipated uses or disclosures of such that are not permitted or required under subpart E of this part.

(4) Ensure compliance with this subpart by its workforce.

§ 164.306 Security standards: General rules.

(b) ***Flexibility of approach.***

(1) Covered entities and business associates may use any security measures that allow the covered entity or business associate to reasonably and appropriately implement the standards and implementation specifications as specified in this subpart.

(2) In deciding which security measures to use, a covered entity or business associate must take into account the following factors:

(i) The size, complexity, and capabilities of the covered entity or business associate.

(ii) The covered entity's or the business associate's technical infrastructure, hardware, and software security capabilities.

(iii) The costs of security measures.

(iv) The probability and criticality of potential risks to electronic protected health information.

§ 164.308 Administrative safeguards.

(a)A covered entity or business associate must, in accordance with § 164.306:

(1)(i) ***Standard: Security management process.*** **Implement policies and procedures to prevent, detect, contain, and correct security violations.**

(ii) ***Implementation specifications:***

(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.**

(B) ***Risk management (Required).*** **Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).**

Overview of Meaningful Use Objectives
Core Measures 15

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) and implement security updates as necessary and correct identified security deficiencies as part of its risk management process.

NIST Assessment Process

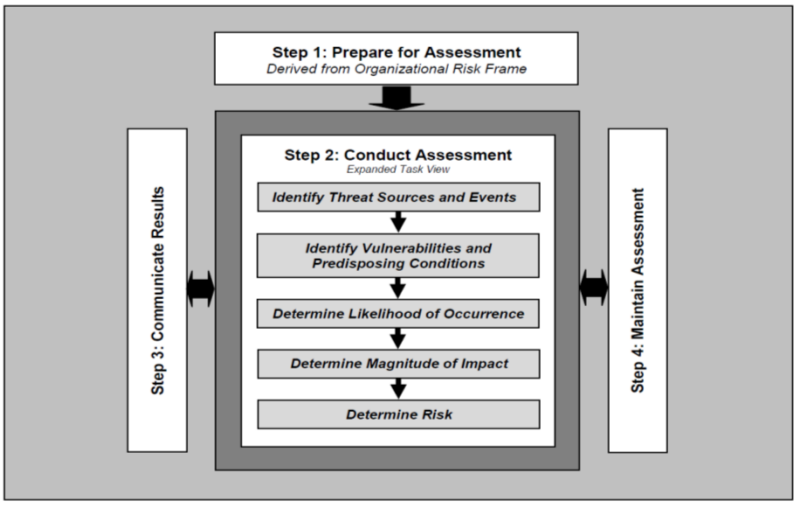

FIGURE 5: RISK ASSESSMENT PROCESS

Terminology

Threat

An adapted definition of threat, from NIST SP 800-30, is "[t]he potential for a person or thing to exercise (accidentally trigger or intentionally exploit) a specific vulnerability." There are several types of threats that may occur within an information system or operating environment. Threats may be grouped into general categories such as natural, human, and environmental.

Vulnerability

Vulnerability is defined in NIST Special Publication (SP) 800-30 as "[a] flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy."

Terminology

Risk

An adapted definition of risk, from NIST SP 800-30, is:

"The net mission impact considering

(1) the probability that a particular [threat] will

exercise (accidentally trigger or intentionally exploit) a particular [vulnerability] and (2) the resulting impact if this should occur . . . . [R]isks arise from legal liability or mission loss due to—

1. Unauthorized (malicious or accidental) disclosure, modification, or

destruction of information

2. Unintentional errors and omissions

3. IT disruptions due to natural or man-made disasters

4. Failure to exercise due care and diligence in the implementation and operation of the IT system."

Terminology

Severity

The severity of a vulnerability is an assessment of the relative importance of mitigating/remediating the vulnerability. The severity can be determined by the extent of the potential adverse impact if such a vulnerability is exploited by a threat source.

Likelihood

The likelihood of occurrence is a weighted risk factor based on an analysis of the probability that a given threat is capable of exploiting a given vulnerability (or set of vulnerabilities). The likelihood risk factor combines an estimate of the likelihood that the threat event will be initiated with an estimate of the likelihood of impact (i.e., the likelihood that the threat event

Impact

The level of impact from a threat event is the magnitude of harm that can be expected to result from the consequences of unauthorized disclosure of information, unauthorized modification of information, unauthorized destruction of information, or loss of information or information system availability.

Terminology

Risk

Risk can be understood as a function of:

1) **the likelihood of a given threat triggering or exploiting a particular vulnerability, and**
2) **the resulting impact on the organization.**

This means that risk is not a single factor or event, but rather it is a combination of factors or events (threats and vulnerabilities) that, if they occur, may have an adverse impact on the organization.

NIST Risk Model

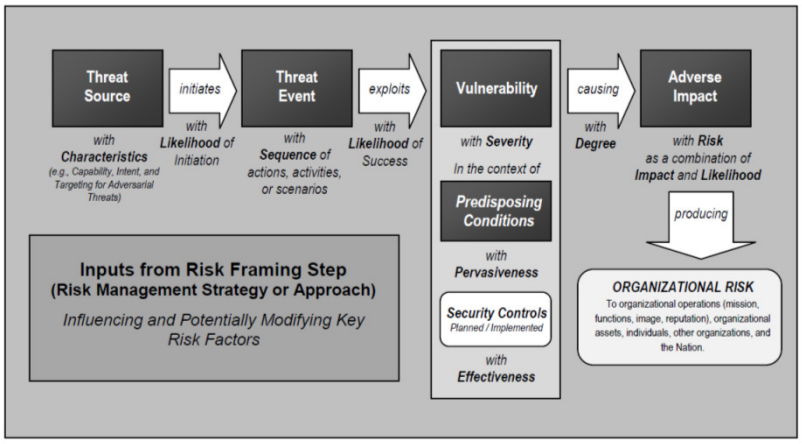

FIGURE 3: GENERIC RISK MODEL WITH KEY RISK FACTORS

Resources

OCR Guidance on Risk Analysis Requirements under the HIPAA Security Rule
http://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html

U.S. Department of Health and Human Services (HHS) The Office of the National Coordinator for Health Information Technology (ONC) - Security Risk Assessment (SRA) Tool
https://www.healthit.gov/providers-professionals/security-risk-assessment

National Institute of Standards and Technology - HIPAA Security Rule Toolkit
https://scap.nist.gov/hipaa/

Resources

NIST Special Publication 800-53A - Guide for Assessing the Security Controls in Federal Information Systems and Organizations

http://www.nist.gov/itl/csd/risk-092011.cfm

NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems and Organizations*.

http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

https://web.nvd.nist.gov/view/800-53/Rev4/home

US Department of Homeland Security Cyber Security Evaluation Tool

https://ics-cert.us-cert.gov/Downloading-and-Installing-CSET

Vulnerability Assessment

A vulnerability assessment involves identifying and quantifying resources residing on a network, then identifying and prioritizing any vulnerabilities or potential threats to each of these resources.

Vulnerability analysis consists of several steps:

- Defining and classifying network or system resources
- Assigning relative levels of importance to the resources
- Identifying potential threats to each resource
- Developing a strategy to deal with the most serious potential problems first
- Defining and implementing ways to minimize the consequences if an attack occurs.

(© TechTarget)

Selected Tools

Nessus - Nessus has been deployed by more than one million users across the globe for vulnerability, configuration and compliance assessments. Nessus prevents network attacks by identifying the vulnerabilities and configuration issues that hackers use to penetrate your network. Aprox. $3,000/year.
https://www.tenable.com/products/nessus-vulnerability-scanner

NMAP - Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Free.
https://nmap.org/

Last Slide

If you don't know where your ePHI resides and flows, you don't know how to protect it.

As such, you don't know the level of risk you are under from sources of threats.