SANS Institute
Information Security Reading Room

Risk Analysis for HIPAA Compliancy

Chris Ralph

Risk Analysis for HIPAA Compliancy

GIAC HIPAA Security Certificate (GHSC)

Practical Assignment version 1.0

Submitted January 6, 2005

By: Chris Ralph

Abstract

This document describes the policy and procedure established by a small hospital, GIAC Health, for meeting the Risk Analysis Administrative Safeguard requirement for HIPAA compliancy. It also includes, in the section 'Assignment 2', a brief explanation of GIAC Health's interpretation of the Risk Analysis required implementation standard.

Assignment 1 – Definition of the Environment

GIAC Health is an independent, eighty-bed hospital with a single location, specializing in acute care and sports medicine. Nearly seventy-five resident physicians and nurses (across three shifts) use the Emergency Department Management application (EDM) from Meditech™. The EDM system runs entirely on Microsoft Windows 2000 servers and is the single, central location for patient information (electronic Protected Health Information). The rest of GIAC Health's IT infrastructure consists of three additional Windows 2000 servers providing Active Directory (AD) services & DNS, email, file & print services, and two Red Hat Linux version 9 hosts--one running Snort 2.0 for network-based IDS watching the Meditech servers, nMap, & Nessus, and one Syslog server providing a central logging facility for the Snort box and the perimeter security appliances. Internet access is available from any PC for authorized users and is provided via a leased T-1 circuit to a local ISP. The internal network uses private (RFC 1918) statically-assigned IP addresses and is protected from the threats of the Internet by a combination of a Fortinet FG-200 IDP appliance and a Cisco PIX 515E firewall performing network address translation (NAT) and port address translation (PAT). The PIX is configured to allow only SMTP traffic from the Internet to the SMTP server on the inside network. HTTP, HTTPS, SMTP, DNS, and FTP are allowed outbound as documented in the hospital's security policies. The FG-200 sits in-line behind the PIX and inspects all inbound and outbound traffic for malicious content and enforces GIAC Health's Acceptable Use Policies via a subscription-based URL and content filtering service. Both devices send logging data to a central syslog and security event management host on the internal LAN.

The MIS department is small and is directed by the CIO who is also the assigned HIPAA Security Officer. The Network Manager is responsible for the infrastructure gear for the LAN as well as Internet access and the two Linux boxes. The System Administrator is responsible for the Active Directory domain and the Windows servers including the Meditech system and data backups. A single PC Support Technician operates the help desk and is responsible for end-user support, PC provisioning & support, anti virus and other non-Meditech applications running on the PCs.

Assignment 2 – Explanation of Risk Analysis Implementation Specification

The overall objective of a HIPAA risk analysis is to document the risks that threaten to negatively impact the confidentiality, integrity, or availability of

electronic protected health information and determine the appropriate safeguards to bring the level of risk to an acceptable and manageable level. It doesn't make sense to blindly spend money and resources on security controls and safeguards without first knowing exactly what it is that we're protecting, what we're protecting it from, what its weaknesses are, and the potential magnitude of loss (single loss expectancy (SLE)) due to an exposure. For example, it is not 'appropriate' to spend $50,000.00 per year on safeguards to protect the privacy of something when the annualized loss expectancy (ALE) or impact to business would not exceed $10,000.00. The choices of safeguards should be based on actual risks to actual assets that have some value to the organization. The confidentiality, integrity, and availability of an asset is what we're protecting; threats are what we're protecting the asset from, the weaknesses are termed 'vulnerabilities', and the potential magnitude of loss or impact describes the 'value' or importance of confidentiality, integrity, and availability of the asset to the organization. Risk is therefore a function of the value or criticality of an asset, the likelihood of and potential harm from threats to the asset, and the vulnerabilities of the systems that incorporate the asset to the threats.

Risk analysis is a required implementation specification under the Security Management Process standard of the Administrative Safeguards portion of the HIPAA Security Rule. Covered entities will benefit from an effective Risk Analysis and Risk Management program beyond just being HIPAA compliant. As described previously, the results of a risk analysis will help to show a return on investment from security expenditures and avoid haphazard spending that does not map to specific risks to patient data. On-going risk analyses will keep the risk management effort focused in the right direction and facilitate effective and efficient use of limited resources to protect the confidentiality, integrity, and availability of electronic protected health information as required by HIPAA.

Assignment 3 – Policy[1]

1.0 Purpose

To state GIAC Health Executive Management's position on Risk Analysis and Security Testing and to empower GIAC Health InfoSec staff and assigned Security Officer to periodically conduct the security test and Risk Analysis to ensure that an accurate and timely representation of threats, risks, vulnerabilities, and safeguards to electronic Protected Health Information is maintained. This information will be used to ensure that appropriate safeguards are in place and that risks are documented and kept to an acceptable and manageable level.

2.0 Scope

Risk Analyses and accompanying security testing will be conducted periodically on all GIAC Health information systems that store, process, receive, or transmit individually identifiable patient information a.k.a. electronic Protected Health information. Risk Analyses may be conducted by GIAC Health's assigned Security Officer and/or InfoSec Dept. staff authorized by the Security Officer

[1] http://www.sans.org/resources/policies/Risk_Assessment_Policy.pdf

and/or a reputable, qualified third party selected and authorized by the Security Officer.

2.1. Applicable information systems for testing/assessing may include: servers, operating systems, applications, databases, PCs, network infrastructure equipment (routers, switches), processes & procedures, and personnel.

3.0 Policy

Risk Analysis is required for compliance with the HIPAA Security Rule for Administrative Safeguards and hereby mandated by GIAC Health Executive Management. A Risk Analysis will be conducted periodically, at the discretion of and under the supervision of, the assigned Security Officer but at least annually and when a significant change is made to the computing infrastructure, policies, procedures, or applications that may impact the security posture and/or current risk profile of GIAC Health. The entire process will be documented along with identified risks. Each risk will be reviewed by the Security Officer and Executive Management Team and either:

3.1. Accepted – The risk is determined to not present a significant danger to the confidentiality, integrity, or availability of ePHI due to the improbability of an exposure or the negative impact of an exposure is less than the cost of mitigation. The risk will remain documented, will be reviewed again during the next risk analysis, but will not be mitigated.

3.2. Mitigated -- The risk is determined to present a reasonable danger to the confidentiality, integrity, or availability of ePHI. Reasonable and appropriate controls/safeguards will be selected to mitigate the risk. The risk will be documented and the safeguard evaluated during the next risk analysis or security test.

3.3. Transferred – The risk cannot be reasonably and appropriately mitigated but could have a negative financial impact should an exposure occur. The financial risk to GIAC Health will be minimized with the purchase of an insurance policy that directly adequately addresses the risk and the cost of the exposure.

3.4. Expectations:

3.4.1. Business Impact – The testing is being conducted in an effort to take a proactive approach to threat mitigation and ultimately minimize the impact to business and patient care provided by GIAC Health. Executive Management expects that the risk analysis team will exercise due care in minimizing the business impact of the testing as well. This will include planning and scheduling in advance any potential or required system downtime and meetings with the appropriate system owners.

3.4.2. Scope of Work – The risk analysis must provide "*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*"[2] in order to comply with the

[2] HIPAA Final Security Rule §164.308(a)(1)(ii)(A) published: February, 2003

HIPAA Standard. Executive Management expects that the security testing and risk analysis will include at a minimum:

3.4.2.1. Inventory & classify assets
3.4.2.1.1. As described under section 2.0 'Scope', this must include all assets/systems that store, process, or transport ePHI
3.4.2.2. Identify all threats to the privacy, integrity, or availability of ePHI that have a reasonable probability of occurrence and/or would cause serious impact
3.4.2.3. Perimeter security evaluation
3.4.2.3.1. Penetration test
3.4.2.3.2. Modem survey
3.4.2.4. Review existing policies & procedures
3.4.2.5. Test enforcement of policies
3.4.2.6. Review previous risk analysis reports
3.4.2.7. Vulnerability scans of systems that store, process, or transport ePHI
3.4.2.8. Wireless network access survey
3.4.2.9. Evaluate existing security controls—physical, technical, and operational
3.4.2.10. Assess the training effectiveness and awareness of GIAC Health's workforce

3.4.3. Recommendations – It is expected that the risk analysis report will be reviewed by the Security Officer and recommendations will be made for appropriate safeguards to mitigate all of the identified risks.

4.0 Risk Analysis Process

See the section 'Assignment 4 – Procedures' for specific procedures describing the execution of the Risk Analysis

5.0 Enforcement

GIAC Health takes compliance with HIPAA and other federal and state regulations and the privacy of patient health information very seriously. All employees of GIAC Health are expected to comply with the policies set forth. Violation of this policy may result in disciplinary action up to and including termination of employment. Contractors and vendors are expected to comply with this policy. Violation will represent a breach of contract and may result in immediate termination of contract.

6.0 Revision History

Version 1.0.0 January 1, 2005
Effective January 1, 2005

Assignment 4 – Procedures (Option B)

The Risk Analysis (RA) process for GIAC Health is modeled after the methodology and guidelines published by the National Institute of Standards and Technology (NIST) in the Special Publication 800-30 'Risk Management Guide for Information Technology Systems'. This provides a standard framework for consistency and follows generally-accepted best practices upon which the HIPAA

standards are based. The overall process is comprised of seven steps that begin after the initial project planning phase. This document describes the tasks required to complete each of the steps and the role within GIAC Health that will be responsible for the completion of each step.
The process will start with a kick-off meeting including the entire risk analysis team to establish a schedule for the RA that will include interviews with key department heads and vulnerability testing of systems that could potentially cause brief periods of system downtime. The Dept. Heads will be notified two weeks in advance of scheduled interviews and vulnerability testing of systems that impact their department. The RA team will be directed by the assigned HIPAA Security Officer and will consist of the Network Manager, System Administrator, and PC Support Tech.

Objectives

The objective of the RA is to identify and document all threats to confidentiality, integrity, or availability of patient information and gauge the probability and potential impact of each threat based upon vulnerabilities in the systems. The effectiveness of existing safeguards in mitigating these risks will be measured and documented and informed decisions will be made regarding the best way to address residual risk.
Due to the limited resources available and minimal complexity of GIAC Health's environment, a qualitative risk analysis will be performed based on a relative scale of 1 to 5 values as opposed to quantitative based upon dollar values, Annualized Rates of Occurrence, Loss Expectancies, and Exposure Factors.

Step 1 – Inventory & Classify Assets

The System Administrator is responsible for reviewing, auditing, and updating the list of critical assets and dependencies including documenting interfaces into each asset, the role of each asset, and the users and data owners. A critical asset is a database, application, service, or file system (including backups on removable media) that processes or stores ePHI or is required to provide patient care. A dependency is a system that is required to house, protect, or provide access to the critical asset.

- Validate the current system inventory by conducting a scan of the network IP subnet using NMAP.
  - Command syntax: *nmap –sT –O 10.1.1.1-254 –v –oN scanresults.txt*
  - Investigate discrepancies and update documentation if necessary
- Interview the Department Head and/or data owner for each critical asset to capture the following information:
  - Criticality of the asset to the department's business and patient care objectives
    - Use the attached Asset Classification Worksheet to assign relative values on a 1 to 5 scale to the importance of confidentiality, integrity, and availability for each asset.
  - Future plans for modifications, upgrades, or replacement of current asset or dependencies

        - Any changes or planned changes to the way that the asset is used and accessed and authorized users
        - What other systems and/or departments use, access, depend upon the asset
    - Document, in the Asset Classification Worksheet, the systems/dependencies (hardware & software) required to support the asset along with the role that each plays
        - These systems will be tested for vulnerabilities in step 3
            - Servers, operating systems, applications, network devices, PCs, client application
    - Document, in the Asset Classification Worksheet, the person responsible for the asset—for example, the data owner

Step 2 – Document Likely Threats to Each Asset

The Security Officer is responsible for this step and should enlist input from every team member. Threat sources can be environmental (power failure, climate control failure, hazardous material spill), natural (blizzard/ice storm, hurricane, flood), or human (denial of service attack, accidental data corruption or deletion, disgruntled employee, vandal).

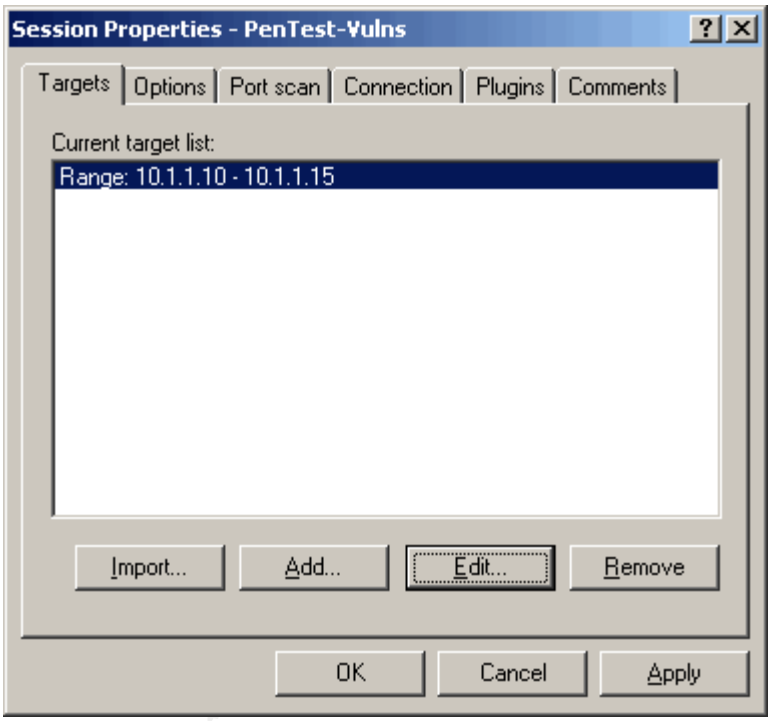
- Complete a Threat Matrix Worksheet (attached) for each critical asset. Use the 1 to 5 scale to represent the value for each parameter
    - Qualitatively assess the likelihood of each threat based upon: climate & weather patterns, value of the asset to the threat source (motivation), capability of the threat source, accessibility of the asset, and susceptibility of the asset to the threat source
    - Qualitatively assess the potential impact that each threat source could have on the confidentiality, integrity, and availability of the asset

Step 3 – Vulnerability Assessment

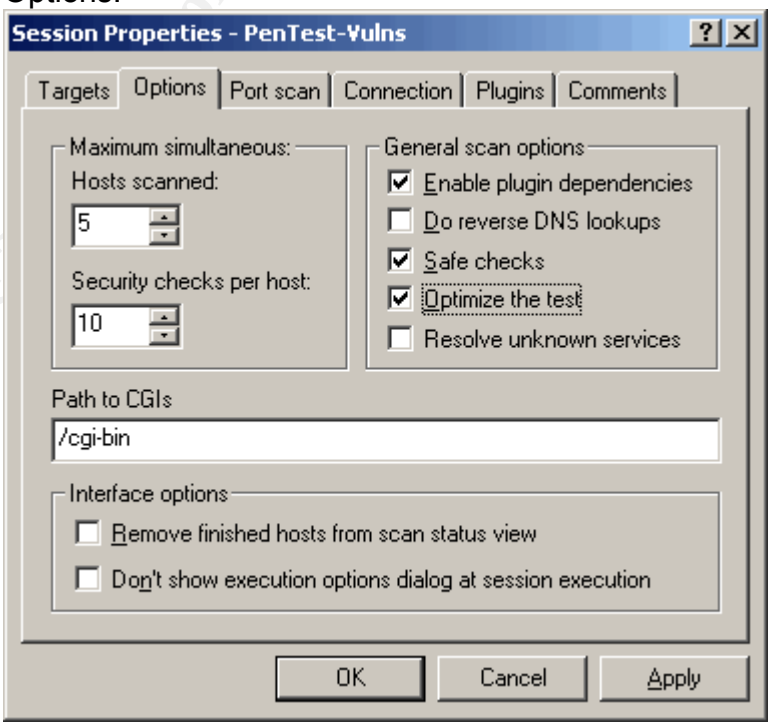
The System Administrator is responsible for this step because this involves security testing of servers, operating systems, and applications. Nessus is the tool used to scan for technical vulnerabilities and is capable of crashing or freezing systems because in many cases, actual exploit code is run against the target system. This scanning will be performed during the time periods scheduled during the planning phase so that department heads can be prepared for possible periods of system downtime. All tests, observations, & results must be documented.

The Nessus daemon is running on the Red Hat Linux Snort IDS host. It is accessed and controlled using the Nessus Windows client—NessusWX already installed & configured on the System Administrator's PC.

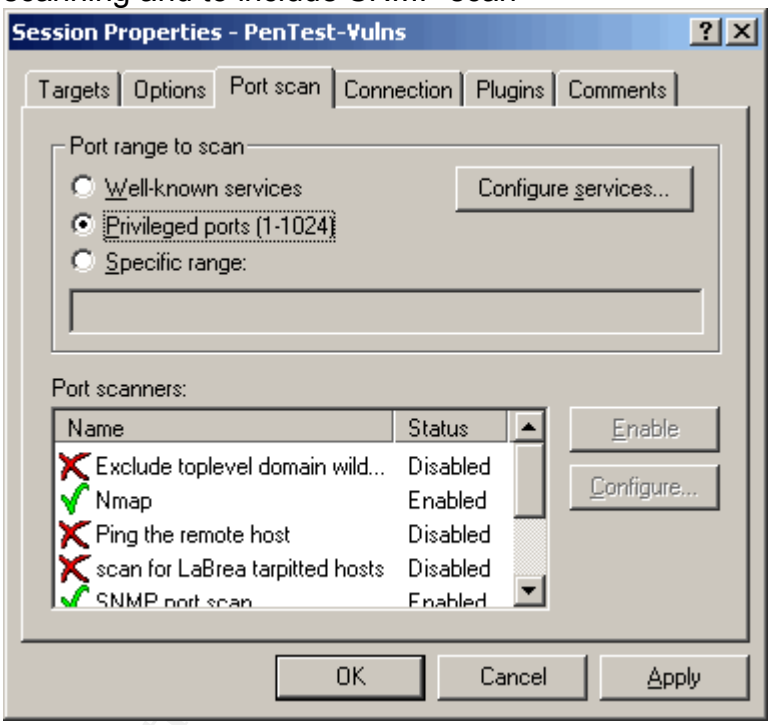
- Contact Meditech for updated list of known vulnerabilities and versions of latest stable patches
- Scan servers for vulnerabilities
    - Verify the proper Nessus scan configuration in the properties of the session within NessusWX.
        - Targets: should include IP addresses of all servers storing or processing ePHI



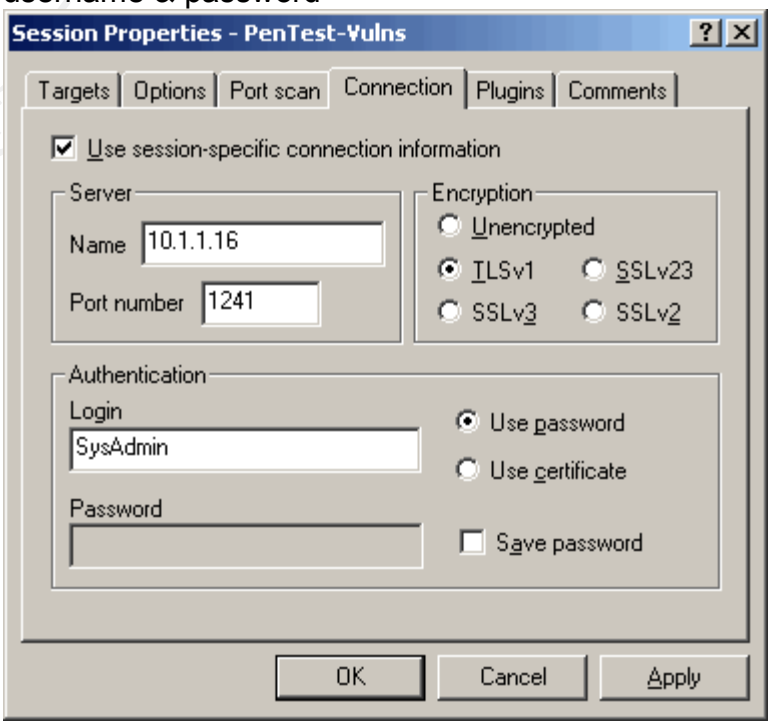
Options:



- Port Scan: Configure Nessus to use Nmap for port scanning and to include SNMP scan

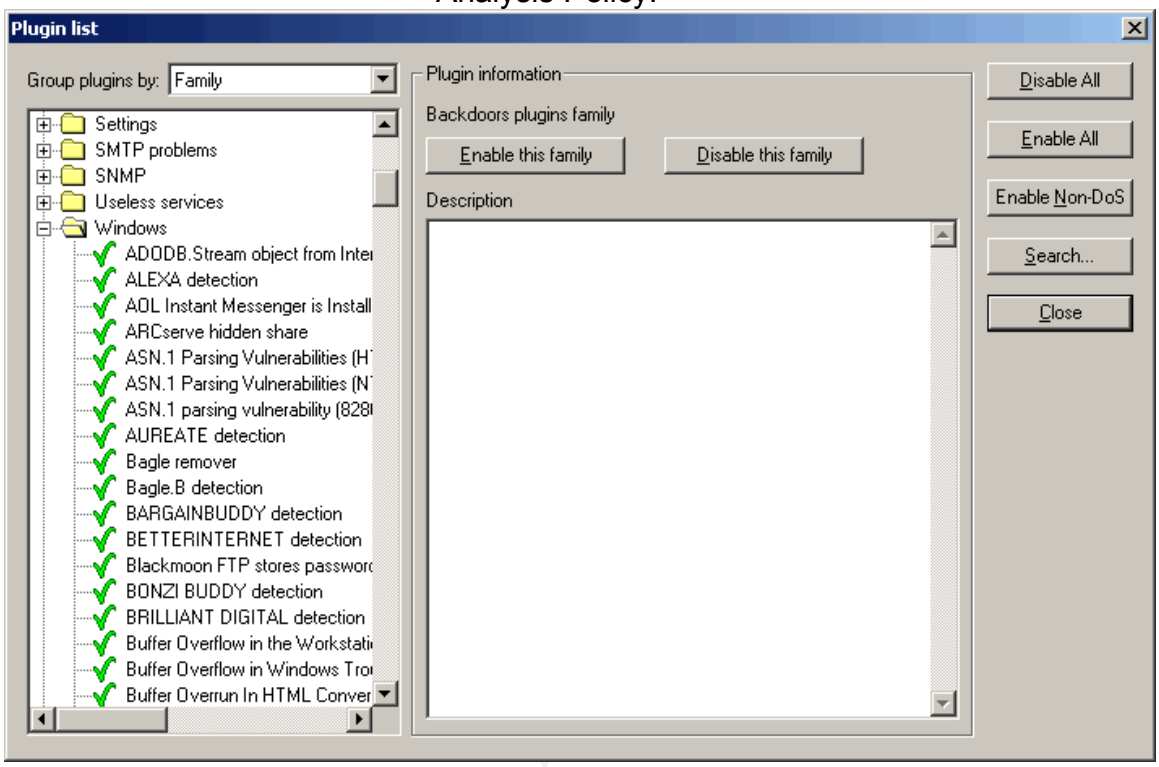


- Connection: enter the IP address of the Nessus server running on the IDS box. Enter SysAdmin username & password



- Plugins: On the Plugins tab, click 'Select Plugins'. Then select 'Enable Non-DoS. This will prevent many of the plugins that might crash a system.

Minimizing impact to daily business during the security test is a requirement stated in the Risk Analysis Policy.



- When the warning screen pops up asking if you want to enable all port scanners as well, select NO to save the choices you made earlier

- Click 'apply' on the session properties screen to save your changes (if you made any) then double-click the session icon to start the vulnerability scan. Scanning the servers will take a while.
- When the scan is complete, save the report in HTML format. This will save useful http links in the report that can be used to get more information on particular vulnerabilities

Step 4 – Evaluate Current Safeguards

This step will map current safeguards to the risks that they were implemented to mitigate and measure their effectiveness. The Network Manager is responsible for the completion of this step.

- Penetration Test – engage a trusted 3rd party to conduct security testing from outside the network (Internet) to validate the configurations of the Internet access router, firewall, and network IDS and provide a report of the results

        - The penetration test should a modem survey (war dial) to identify all modems that are configured to auto-answer incoming calls.
    - Review previous risk analysis reports and verify that previously identified risks are adequately addressed in policy and mitigated by safeguards.
    - Review policy & procedure documents—ensure that all documented risks and threats listed in the Threat Matrix with an impact and/or likelihood rating of 3 or higher are addressed in policy and procedures for safeguards. List the appropriate document name in the 'Safeguards' column of the Threat Matrix Worksheet.
    - Wireless LAN Access Point Survey – Use a laptop computer with an 802.11b/a wireless LAN adapter configured with NetStumbler[3]. Current policy dictates that wireless LANs are not used by GIAC Health. Any access points detected on the GIAC Health network are in violation of policy.
    - Validate operational and physical security safeguards
        - Ensure that network documentation is accurate & up-to-date
        - Review logs from firewall, IDS, web usage, email system, login monitors. Are current procedures for Security Activity Review adequate?
        - Review physical access logs to server room. Verify that physical access to servers cannot be achieved without a proximity card and that all access is being properly recorded
        - Review anti virus standards and configurations on PCs and servers. Signature updates must be automatic and occur daily.
        - Review Help Desk logs for indications of trends or malicious code on PCs
        - Document all findings, concerns, & corrective actions
    - Document safeguards in the Threat Matrix worksheet by listing the specific control and/or process in the 'safeguards' column for each risk that it mitigates

Step 5 – Document Risks

All of the information gathered from the previous 4 steps must be aggregated and correlated to determine actual risks to the assets and to the organization. Here we will incorporate the results of the vulnerability scans, security tests, and safeguard evaluation into the Threat Matrix to gain more accurate results of threat likelihood and impact potential. A numerical 1 to 5 scale is used where 1-2 represents a low risk that may be acceptable, 3 represents a medium risk that should be mitigated through strategic planning of safeguards and 4-5 represents a significant and immediate danger that should be corrected as soon as possible. A threat is a greater risk if vulnerabilities exist that the threat source is capable of exploiting. The Security Officer will oversee the consolidation and correlation of the data gathered by the RA team.

[3] http://www.netstumbler.com/downloads/

- Review the Nessus report. Many of the Holes, Warnings, and Notes reported by Nessus will be due to missing OS patches or software updates. These should be listed in a separate report and given as an action item to the System Administrator. Other vulnerabilities may be flagged as Holes or Warnings because Nessus assumes that it is scanning from an untrusted perspective of the network. For example, open NetBIOS ports are normal for Windows servers when seen from the same trusted network. These should be flagged as false positives and filtered out. Remaining Holes & Warnings should be used to adjust the likelihood and/or impact values in the Threat Matrix Worksheet accordingly.
    - For each documented risk to each asset in the Threat matrix, identify vulnerabilities that could be exploited by that threat and increase the likelihood value of the threat based upon the criticality of the vulnerabilities.
- Apply information from Safeguard Evaluation (step 4) to Threat Matrix
    - Some of the vulnerability and threat pairings may be mitigated by current or planned safeguards. If a current safeguard is deemed effective in step 4, then adjust the likelihood value for that risk accordingly
    - Note any planned safeguards
- Review Penetration Test report
    - External human threats are mitigated primarily by the network perimeter security controls—PIX firewall and Snort IDS. The Penetration Test report will indicate the effectiveness of those controls. Incorporate this information into the Threat Matrix in a similar fashion to the previous step.

Step 6 – Recommend Appropriate Safeguards

Risks that are still listed as a 3 or higher in the threat matrix require recommendations for mitigation. The Security Officer will oversee this report of recommendations. The recommendations should be reasonable and appropriate to enforce GIAC Health policies while reducing the specific risks to a reasonable and manageable level. In many cases, the safeguards will involve creating or modifying processes and/or training employees.

- Itemize risks in a separate document that are listed in the Threat Matrix as a 3 or higher.
- For each risk, describe the recommend safeguard and an estimated total cost to implement and maintain the safeguard.

The asset classification data will be useful for this to ensure that the safeguard is protecting what is important to the specific asset---confidentiality, integrity, or availability.

Step 7 – Create Report of Results

The Security Officer is responsible for compiling all of the data and reports from the previous steps into two separate reports. One report will be an executive report and will include the Asset Classification worksheet, the Threat Matrix worksheets, the recommended safeguards, and an executive summary. The other report will be a compilation of all of the documented data from all of the previous steps including the Penetration Test report, Nessus vulnerability scan report, the executive report, the wireless LAN survey results, and Nmap scan results. This data will be saved together in electronic format and reviewed again during the next risk analysis to ensure that GIAC Health's Risk Profile is improving rather than worsening.

Appendix

Asset Classification Worksheet				Use scale of 1-5 for values		
	GIAC Health		Date:			
	Risk Analysis Team members:			Criticality		
ID#	Asset Name	Asset Owner	Dependant on these systems:	Confidentiality	Integrity	Availability
1						
2						
3						
4						
5						
6						
7						
8						
9						
10						
11						
12						
13						
14						
15						
16						
17						
18						
19						
20						
21						
22						
23						
24						
25						

Threat Matrix Worksheet					
GIAC Health	**Date:**	**Asset ID:**			**Asset Name:**
Risk Analysis Team members:					
Threat Sources	**Likelihood**	**Impact**			**Safeguard**
HUMAN		**Confidentiality**	**Integrity**	**Availability**	
Explosion					Contingency plans
Burglary/Extortion					User awareness and physical access controls
Vandalism					User awareness and physical access controls
Bomb Threat					Emergency operations procedures
Terrorism					User awareness and physical access controls
Riots/Civil Disturbance					User awareness and physical access controls
Work Stoppage					Emergency operations procedures
Data Entry Error					Auditing
Improper Handling of Sensitive Data					User awareness training, physical & technical access controls
Unauthorized Access to Data/Theft					Physical & technical access controls, firewall, IDS
Malicious Damage/Destruction of Software/Hardware					Physical & technical access controls, firewall, IDS
Unauthorized Physical Access					Physical access controls, user awareness, visitor sign-in procedures
Unauthorized Modification of Software/Hardware					Access control & auditing procedures
Virus/Worm/Malicious code					Physical & technical access controls, firewall, IDS, User awareness training, Workstation security
ENVIRONMENTAL					
Power Failure/Fluctuations					Backup power, UPS
HVAC Failure					Redundancy, contingency plans
Hardware Malfunction					H/W redundancy, incident response
System Software Failure					Incident response, contingency plans
Communication System Failure					H/W redundancy, emergency operation mode
Flood/water damage					Contingency plans, emergency operation mode, disaster recovery
Hazardous Waste					Contingency plans, emergency operation mode, disaster recovery
Nuclear Fallout					Contingency plans, emergency operation mode, disaster recovery
NATURAL					
External Flooding					Contingency plans, emergency operation mode
Internal Fire					Contingency plans, emergency operation mode, disaster recovery

External Fire					
Seismic Damage					Contingency plans, emergency operation mode, disaster recovery
Wind/Hurricane/Tornado Damage					Contingency plans, emergency operation mode, disaster recovery
Snow/Ice Storm					Contingency plans, emergency operation mode, disaster recovery

References:

HIPAA Security Implementation Version 1.1 – SANS Step-By-Step Series – SANS Press Copyright 2004

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

http://www.sans.org/resources/policies/Risk_Assessment_Policy.pdf

Nessus Network Auditing by Renaud Deraison, Jay Beale, HD Moore, Noam Rathaus, et al. Syngress Publishing, Inc. Copyright 2004

Last Updated: October 31st, 2020

Upcoming SANS Training

Click here to view a list of all SANS Courses

SANS Sydney 2020	**Sydney, AU**	**Nov 02, 2020 - Nov 14, 2020**	**Live Event**
SANS Secure Thailand	**Bangkok, TH**	**Nov 09, 2020 - Nov 14, 2020**	**Live Event**
APAC ICS Summit & Training 2020	**Singapore, SG**	**Nov 13, 2020 - Nov 28, 2020**	**Live Event**
SANS Community CTF	**,**	**Nov 19, 2020 - Nov 20, 2020**	**Self Paced**
SANS Local: Oslo November 2020	**Oslo, NO**	**Nov 23, 2020 - Nov 28, 2020**	**Live Event**
SANS OnDemand	**OnlineUS**	**Anytime**	**Self Paced**
SANS SelfStudy	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**