HIPAA Risk Analysis

By: Matthew R. Johnson

GIAC HIPAA Security Certificate (GHSC)

Practical Assignment

Version 1.0

Date: April 12, 2004

Table of Contents

Abstract

This paper discusses GIAC Health, a small medical practice that falls under the designation as a covered entity and is subsequently regulated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The scope of this document is to explain the policies and audit procedures that GIAC Health is required to undergo in order to comply with the Risk Analysis implementation specification under the Security Management Process standard in the HIPAA Security Rule. This document will give a brief overview of GIAC Health's operating logistics, applications, and network topology. The Risk Analysis implementation specification will be briefly discussed within the context of the Security Management Standard which it falls under. A sample policy is outlined that ensures compliance in a reasonable and appropriate manner in reference to the HIPAA standard. A series of steps will then be outlined for GIAC Health managers and security consultants to conduct a simple audit of Risk Analysis procedures, documentation, and post-assessment remediation planning of InfoSec staff performing the assessments to gauge compliance with the policy.

Assignment 1 – Define the Environment

GIAC Health is a small specialized medical practice with a single location in California's Central San Joaquin Valley. GIAC Health is owned jointly by a local hospital and a large physician's medical group. GIAC maintains a dedicated T-1 data line to the partner hospital for scheduling surgeries, sharing Protected Health Information (PHI), and saving off-site backups. The T-1 operates on a private network and utilizes a Cisco PIX 515e Firewall to a Cisco 1700 series router. GIAC Health has 34 Workstations all running Microsoft Windows 2000 Professional that connect to a Windows 2000 Server for active directory services, authentication and file sharing. The practice management software used by GIAC Health is The Medical Manager Suite by WebMD, Inc. The Medical Manager software is running on a dedicated UNIX server with SCO OpenServer 5.0.7 as the operating system. Workstations access the Medical Manager system using SSH and a thin client running on their PC. GIAC Health maintains a DSL line to the internet protected by a Netscreen 50 Firewall and a Cisco 1700 series router. This firewall does not utilize port address forwarding since there are no public web or email services running on the internal servers. Only one public IP address is utilized by GIAC Health and it is assigned to the Netscreen firewall for Port Address Translation of internal machines to access the internet.

Assignment 2 – Explanation

Overview: HIPAA and the Security Rule

HIPAA is a federal law which legislates the activities of the Health and Medical industry in an effort to protect and simplify the process of managing, sharing, and storing critical and private patient information. Organizations that fall under the HIPAA legislation are referred to as Covered Entities (CE). The Security Rule comprises one part of the overall HIPAA legislation and specifically addresses issues concerning the confidentiality, availability and integrity of electronic individually identifiable health information. The Security Rule structure categorizes 18 standards into three safeguards: Administrative, Technical and Physical. These standards address issues in a generic, non-vendor specific manner, allowing companies latitude in implementation decisions leading to compliance of the standards. Each standard may include implementation specifications defining specific areas of the standard in greater detail that need to be addressed in order to comply with the standard.

Standard: Security Management Process

The Security Management Process is one of 9 standards under the Administrative Safeguards of the Security Rule. The purpose of the Security Management Process standard is to enforce a proactive rather than reactive security posture through planning, prevention, containment and documentation of policies and procedures that identify and address potential security violations to ePHI. These goals are accomplished through on-going assessment,

management and review of technologies, system activity, and anomaly detection of information systems.

Implementation Specification: Risk Analysis (Required)

The Risk Analysis Implementation Specification is a required specification under the Security Management Process. The Risk Analysis must be documented and implemented in a reasonable form that can be justified in the event of an audit. The Risk Analysis implementation specification is described within the final Security rule as follows in §164.308:

> (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.[1]

The burden for compliance of the Security Management Process standard and the Risk Analysis implementation specification becomes greater for the CE when the previous text is taken into context of regulations adjoining §164.308(a) and the greater scope of the Security Rule; for instance §164.308(e) states:

> (e) *Maintenance.* Security measures implemented to comply with standards and implementation specifications adopted under §164.105 and this subpart must be reviewed and modified as needed to continue provision of reasonable and appropriate protection of electronic protected health information as described at §164.316.[2]

The Covered Entity must understand that they cannot conduct a one time assessment to appease the regulation but must conduct regular assessments when technologies and practices are "reviewed and modified" to "continue provision of reasonable and appropriate protection". The only part that is remotely open to interpretation would be the "as needed," which may not be defined until precedence is set in a court of law. However, with the rapid rate which technology changes and vulnerabilities are exploited and discovered, we can be sure the definition of "as needed" will not be a substantial amount of time.

Assignment 3 – Policy

The following policy establishes a requirement within GIAC Health that supplements existing InfoSec best practices guidelines with a more concrete outline of necessary actions needed to comply with HIPAA Risk Analysis

[1] http://www.cms.hhs.gov/hipaa/hipaa2/regulations/security/03-3877.pdf
[2] Ibid.

regulations. The scope and frequency in which systems are assessed is ultimately at the discretion of GIAC InfoSec managers based on the perceived threat to their security posture relative to vulnerabilities within the technology landscape.

Risk Analysis Policy

1.0 Purpose

This policy outlines the requirements for conducting periodical risk analysis and security assessments on GIAC Health networks, systems, and operating procedures. Adherence to this policy will ensure minimal negative impact to operations and system performance during assessments and will satisfy compliance with the HIPAA Risk Analysis implementation specification.

2.0 Scope

The scope of this policy includes reviewing all systems, networks, procedures and operations related to GIAC Health that contain, manipulate, or access electronic protected health information. This policy includes all present and future personnel, equipment, systems and vendors that access or store GIAC Health information.

3.0 Policy

Risk Analysis is a critical part of GIAC Health's commitment to information security and the absolute protection of GIAC patient information. The Risk Analysis is a required implementation specification under HIPAA regulations and must be performed and documented on an on-going basis to ensure compliance. Under this policy, items covered within the scope of the policy will be reviewed for known vulnerabilities. In addition, operational procedures will also be assessed to ensure maximum efficiency, security, and patient confidence while maintaining the highest level of confidentiality, availability and integrity to ePHI.

3.1 Vulnerability Assessment Requirements

a. Planning. Personnel conducting the vulnerability assessment will complete a written statement of intent outlining the actions to be taken during the assessment. The statement of intent is required to contain at a minimum; an outline of dates and times in which the assessment will take place, who the contact will be for questions or collateral problems relating to assessment activities, and what specific activities will be included within the assessment.
b. Assessment Activities. The scope of the assessment will vary depending on the purpose of the assessment. Under no condition will a regularly scheduled general assessment include less than the following:
    a. Network Discovery
    b. Interviews & Questionnaires

c. Perimeter Analysis. (Extensive attention should be placed on internet or outside facing network devices which can compromise network system security or integrity.)
d. Password Integrity Audits
e. Physical Inspections
f. Wireless Sweeps
g. Firewall and Router ACL reviews
h. Firmware and software vulnerability scans
i. Policy and Procedure Reviews

3.2 Remediation

The remediation phase of an assessment will outline the budget associated with the estimated cost incurred to mitigate physical and technical vulnerabilities. It must include a project plan that prioritizes action points and solutions and identifies responsible parties. The remediation plan must include the results of the discovery scans and document the current topology of the assessed network. All documentation prepared and compiled during remediation planning will be submitted to the InfoSec department manager for review and approval within 14 days following the close of the assessment.

3.3 Service Interruptions

It is common for degradation or interruption of system resources to occur during the course of an assessment. If interruptions are expected, it is the responsibility of InfoSec personnel conducting the assessment to notify all potentially affected staff via email or written memo at a minimum 24 hours before the interruption is to occur.

4.0 Enforcement

This policy will be enforced and executed by InfoSec personnel under the direct guidance of the Chief Security Officer. Delegation of duties in response to remediation will be coordinated by the CSO and accountability for corrective actions will be enforced directly by the director of their respective departments. Any employee violating this policy will be subject to corrective measures and prosecuted under the terms of their individual employment agreements.

5.0 Revision History

Version: 1.0 Initial Release
Revised: April 7, 2004
Effective Date: April 7, 2004
Issued By: Matt Johnson, GIAC Health Systems

Assignment 4 – Option B: Audit

The following audit procedure outlines the necessary steps that the security officer or consultants must take in auditing compliance with the Risk Analysis policy for GIAC Health. The steps below attempt to outline the best method for achieving the stated goals within the policy based on common knowledge of

GIAC Health staff and easily accessible tools that InfoSec personnel may utilize during assessment. This checklist attempts to overview the basics needed to satisfy the requirements of the policy. Additional procedures and checklists for each step would need to be in place to satisfy procedure requirements in order for InfoSec staff to perform the assessment.

Step 1: Network Discovery

The assessment must commence with a network discovery process that identifies applicable devices to be assessed. Tools such as NetRAT[3] or IP Network Browser[4] can be used to discover the network and help identify services that should be tested for vulnerabilities. Additional tools may be used by the InfoSec staff based on specific requirements and training received by the individuals performing the assessment. Network Discoveries should be well documented and included within the remediation plan.

Step 2: Interviews and Questionnaires

Policies and procedures need to be reviewed on a regular basis. Conducting interviews with key stake holders in each department will ensure that best practices are being used when handling and accessing PHI. Questions should be specific to each manager's scope of responsibility. Questions asked should contain at a minimum the questions outlined in the companies interview and questionnaire procedures. Each questionnaire should be printed and included in a report following the assessment. Any areas requiring new or modified procedures should be documented and included in the remediation plan.

Step 3: Assessing the Perimeter

The largest threat of system access from an outside user who is not employed by GIAC Health will come from gateways facing external networks, otherwise known as the perimeter. GIAC Health should only have two network gateways on the perimeter. The first is the T-1 Line to the hospital and the second is the DSL line to the internet. Users on the hospital network should have complete access only to the Medical Manager system on the SCO Unix server. Internet users should have no access to any system on the private network. Access lists, group permissions, active directory group policy objects and organizational units should all be verified to be consistent with the policies and procedures governing access. The only externally accessible IP address in use by GIAC Health is the IP used on the firewall for Port Address Translation (PAT) of external machines to the internet. Policies are in place on the Netscreen Firewall to disallow connections to the IP and to make it appear invisible to the outside users and internet worms. To verify our assumptions regarding the perimeter, a tool such as nmap[5] should be utilized. The following nmap command is used from the internet to verify the network is invisible.

---

[3] http://www.netratsoftware.com/
[4] http://www.solarwinds.net/Tools/Network_Discovery/IP_Network_Browser_PE/
[5] http://www.insecure.org/nmap/

```
# nmap -sS –sU 2.2.2.4

Starting nmap V. 2.54BETA31 ( www.insecure.org/nmap/ )
All 1554 scanned ports on  (2.2.2.4) are: filtered

Nmap run completed -- 1 IP address (1 host up) scanned in
165 seconds
```

The –sS and –sU options are used to check for both UDP and TCP accessibility to GIAC Health's outside IP address.

Step 4: Password Integrity

Weak passwords and password sharing is the largest potential vulnerability to the GIAC Health system that would originate from inside the network. Password sharing can only be discouraged with education and policies that are strictly enforced. Weak passwords on the other hand can be avoided using complex password management. While GIAC health maintains policies to limit weak passwords, during the assessment a tool called RainbowCrack[6] should be utilized to be sure that passwords are hardened. Documentation of findings should be included in the assessment and users in violation of the policy need to be outlined in the remediation plan.

Step 5: Physical Inspection

A physical inspection needs to be included in the assessment. At a minimum, access inspections to facilities and locations containing systems that hold electronic patient information should be performed. Both egress and digress access to these systems should be evaluated for the ability to audit activity. Workstations should be inspected for the presence of unauthorized modems, wireless access points, or USB pen drives. Documentation listing who has keys to what areas of the facility should be reviewed for accuracy and updated if necessary. All findings should be included in the assessment and any violations included in the remediation plan.

Step 6: Wireless Sweeps

A wireless sweep should be conducted using Kismet[7] or Netstumbler[8] to detect the presence of unauthorized wireless networks. For GIAC Health, there should be no wireless networks running within the facility.

Step 7: Firewall and ACL Reviews

Access Control Lists (ACL) on the firewall and routers need to be reviewed to verify resource access is as limited as possible to systems containing ePHI. Any changes or modifications should be documented and included in the remediation plan.

---

[6] http://www.antsight.com/zsl/rainbowcrack/
[7] http://www.kismetwireless.net/download.shtml
[8] http://www.netstumbler.com/

Step 8: Firmware and software vulnerability scans

Nessus Security Scanner[9] or comparable scanner should be utilized to check software systems against known software vulnerabilities and basic security weaknesses. For Microsoft systems, utilities such as windows update and Microsoft Baseline Security Analyzer[10] need to be run to verify they are up to date and ensure that the latest vulnerability patches are applied. For GIAC's SCO Unix system, the latest maintenance pack must be obtained and installed and any other vulnerability patches need to be applied. Systems should be set up to periodically check for updates, so GIAC systems do not have to rely on assessments to stay current. Scheduled patch maintenance needs to be verified during the assessment as well. OS upgrades or major updates necessary for vulnerability patching need to be identified and included in the remediation plan.

Routers and firewalls should be checked for the latest firmware and IOS patches then updated and documented as necessary.

The Medical Manager software should be reviewed for known security issues and any updates to the software modules should be addressed and documented.

Step 9: Policy and Procedure Reviews

Policies and Procedures should be reviewed during the Risk Analysis to ensure they are clear and concise. Procedures overseeing monitoring of logs such as syslog from the firewall, router, or IDS should be consolidated and reviewed frequently using a syslog reporter to make sure anomalous activity can be addressed in a timely manner. Windows security event logs from the Windows servers should be reviewed for repeated failed logins from user accounts. Part of assessing your logging procedures should be to identify who should be watching the logs on a daily basis and verify that they really are. Verify that the processes for reporting anomalous activity is being followed and that the documentation is sufficient and clear on who is accountable. Other policies and procedures affecting overall security and HIPAA compliance should also be reviewed. Procedures addressing Employee training, suspension of user accounts, workstation access and access levels for Medical Manager policies should all be reviewed and revised if necessary. Compliance violations should be documented and reviewed during Risk Analysis. The findings and changes to your Policies and Procedures matrix need to be included in the remediation plan.

Step 10: Remediation Planning

The Remediation and planning phase of the assessment needs to include a project plan outlining assessment findings into a spreadsheet application and categorized by priority and likelihood of compromise due to the impact or significance of the vulnerability. Each finding needs to include a solution and be assigned a responsible party with a target date for remediation. A budget needs

[9] http://www.nessus.org/doc/datasheet.pdf
[10] http://www.microsoft.com/technet/security/tools/mbsahome.mspx

to be included itemizing the cost associated with mitigation of each finding. Supporting documents such as interview questionnaires, process documentation, policies and procedures, topology and discovery maps, and reports from tools and utilities, need to all be compiled into a finalized assessment and presented to the department manager with the remediation plan within 14 days of the completion of the assessment.

References

45 CFR Parts 160, 162, and 164 Health Insurance Reform: Security Standards; Final Rule (HIPAA), Department of Health and Human Services, Office of the Secretary, Federal Register February 20, 2003

NetRAT, Version 2.5 Datasheet, URL: http://www.netratsoftware.com/PDFs/NetRAT_Brochure_2-5Ver2.pdf

IP Network Browser, Solarwinds Network Management. Datasheet, URL: http://www.solarwinds.net/Tools/Network_Discovery/IP_Network_Browser_PE/

NMAP Network Mapper Version 2.52, OpenSource GNU GPL Datasheet, URL: http://www.insecure.org/nmap/

Project RainbowCrack, Zhu Shuanglei, Kingnet Security Inc. URL: http://www.giac.org/practical/GCIH/Mike_Mahurin_GCIH.pdf

Kismet Version 4.01, Mike Kershaw, Kismet Wireless, GNU GPL Datasheet, URL: http://www.kismetwireless.net/documentation.shtml

Netstumbler Version 0.3, W. Slavin, GNU GPL Datasheet, URL: http://www.netstumbler.com/

Project Nessus, Renaud Deraison, GNU GPL Datasheet, URL: http://www.nessus.org/doc/datasheet.pdf

Microsoft Baseline Security Analyzer Version 1.2 Datasheet, URL: http://www.microsoft.com/technet/security/tools/mbsahome.mspx