GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

CLOSING THE GAPS IN SECURITY: A HOW-TO GUIDE

Jody Simmonds

March 22, 2002

Version 1.3

© SANS Institute 2000 - 2002, Author retains full rights.

ABSTRACT

Where and how does the journey to security compliance begin when organizations are faced with new regulations and increased scrutiny? One could choose to throw out the current security program and build a program to meet the requirements of the new laws. Another option is to revise the existing security program to meet the new requirements. This could be a more viable option for many organizations and is the one this paper will address.

As the privacy and security compliance deadlines of federal regulations having widespread impact to the health care industry grow near, many practical "how to get started" resources are available to the health care community. The nonspecific approach taken by the health care industry in the areas of administrative, physical, and technical security allow each step to be tailored to meet the needs of other industries facing new security mandates. The objective of this paper is to present a step-by-step approach for assessing an organization's security strengths and weaknesses when compared to the new standards. Since most practitioners agree the security gap analysis is among the critical first steps towards compliance, this paper will focus on the gap analysis process by answering the following questions:

1. What is a gap analysis?
2. When should a gap analysis be performed and by whom?
3. How should a gap analysis be conducted?

After the analysis is completed, the steps leading to implementation will also be discussed. This paper will attempt to consolidate much of the information available on this topic to serve as a useful guide for others assigned the task of security compliance.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

INTRODUCTION

As efficient service delivery becomes increasingly dependent on the broad accessibility allowed by interconnected networks and the Internet, we are confronted with serious threats to critical technology infrastructures. From unauthorized access to intentionally perpetrated viruses and worms, these threats are constantly evolving and the need for appropriate and effective countermeasures has become critical. Information technology security professionals are facing greater challenges in protecting the nation's critical information infrastructure from today's more sophisticated threats. The need for standardized security measures across the nation's business community and the ability to protect the public's privacy has received the attention of lawmakers. Emerging federal and state security and privacy regulations, such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and Gramm-Leach-Bliley Act of 1999 (GLBA), are placing greater demands on both the public and private sector to protect the confidentiality, integrity, and availability of information assets.

The Health Insurance Portability and Accountability Act and the Gramm-Leach-Bliley Act both contain provisions calling for greater security measures in the health care and financial industries respectively. HIPAA security standards were designed to be technology neutral, flexible and cost-effective for various organizations. Amy Helen Johnson points out in her ComputerWorld article "Gramm-Leach-Bliley: The Next Big Thing?" that HIPAA rules provide the fundamentals for many security situations and that HIPAA is a good standard of security for anyone.[1] These standards will almost certainly have a significant impact on determining security best practices for other disciplines and paving the way for other industries to take a serious look at their security policies, architecture, practices, and procedures.

The September 11, 2001, terrorist attacks on the United States also heightened awareness for security standards. The newly created Office of Homeland Security proposes to work with federal, state, and local, and private organizations to coordinate protection of critical public- and privately-owned information systems within the United States. In January 2002, Senator John Edwards (D-North Carolina) introduced two new cybersecurity bills seeking to increase both government computer security and general education in the field.[2]

Chapter 3 of The 2000 Guide to Health Data Security written by Shannah Koss has defined the key steps an organization should take to get ready for mandated security deadlines as follows:

- Assign initial security responsibilities and drive organizational awareness.
- Undertake a baseline assessment of current security capabilities.
- Conduct a gap analysis between current security and the security required under the new regulations.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Conduct a risk assessment.
- Make risk management decisions based on risk-benefit analyses.
- Identify needed resources both internal and external.
- Develop and revise security policies and processes.
- Validate, revise or design an organization's security architecture.
- Implement the organization's enterprise wide security program.
- Establish corresponding administrative support for all implementation components.
- Establish audit processes and mechanisms.[8]

Establishing an inventory or "baseline" of your current system and comparing it to the new requirements is considered by many as the most critical step towards compliance. It is from this process that an organization's security program will evolve. Here is a closer look at the security gap analysis process.

WHAT IS A SECURITY GAP ANALYSIS?

Before an organization starts trying to change any of its security methods, it needs to answer two questions:

- What security measures are in place today?
- What additional security will be needed to comply with the new regulations?[8]

A gap analysis is certainly not a new concept nor is it restricted to the information security environment. In fact, the gap analysis phase has been considered a necessary first step in project management for all kinds of disciplines. What is a security gap analysis? According to Phoenix Health Systems, HIPAAnote, Volume 12, Number 55, December 5, 2001:

> a security gap analysis is determining the current status of an organization's environment as it relates to compliance with new regulations. To do this, one must first do an analysis of the "baseline" environment, including current computer and communications systems and security-related policies, processes, practices and technology. The scope of effort should include off-site entities as well as on site departments including the existing physical security measures. The deficiencies between the baseline environment and new regulatory requirements are called the "gap." [10]

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Who Should Perform a Security Gap Analysis?

A security gap analysis can be performed either by in-house staff, outsourced to a consulting firm, or by a combination of both. The choice is left to each individual organization depending on business requirements, availability of staff and funding resources. Some organizations may choose to do it in-house in order to save money. Others may simply not have available or trained internal staff resources to conduct the analysis. Regardless of the option chosen, internal IT staff needs to be involved in all facets of the assessment process. If an organization does choose to outsource, a careful review of the contracted company 's references before work begins is strongly suggested.

What Steps Are Involved in the Gap Analysis?

The gap analysis process itself is a comprehensive course of action involving several steps and requiring careful planning to be successful. The initial step is to develop a gap analysis project plan. The purpose of this plan should include, but not be limited to, such topics as the description, purpose, scope, and benefits of the analysis. An organization may require other key elements based on organizational business needs and processes. Once the project plan is developed, the organization is ready to proceed.

Amy Helen Johnson offers these steps in her ComputerWorld article entitled "Gap Analysis 101":

1. Obtain a copy of the regulations with which an organization must comply or write a set of standards that will define the security goals.
2. Define the scope of the analysis. Consider conducting several analyses that focus on different parts of the operation.
3. Collect all of the relevant documents that describe current practices, including privacy policies, security procedures and hardware and software procedural documentation.
4. Take a physical inventory of systems. Auditing software indicates what machines and software are on the network.
5. Conduct interviews to find out what procedures employees actually use.
6. Examine your systems for proper implementation of security measures, paying attention to common problem areas such as configuration settings.
7. Compare current security practices and tools against the standards.
8. Prioritize the gaps, and then implement remedies.[9]

The above-mentioned guidelines offer an excellent starting point for beginning the security compliance process. It is, however, important to define these guidelines further.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The first step towards compliance should be to determine the current degree of security readiness by conducting an assessment of all systems, policies, procedures and practices -- and accompanying it with a security risk analysis. Armed with these results, along with business and financial plans, an organization will be well positioned to develop its security compliance objectives, priorities and implementation plan.[3]

Large-scale security compliance efforts such as HIPAA may cost an organization a considerable amount of money. It is crucial to assess what is already in place before trying to find solutions for meeting the new requirements. To facilitate this process, a checklist matrix would be beneficial. The following "Action Checklist" developed by Phoenix Health Solutions is HIPAA specific to some degree. For the most part, it is applicable to any industry and can be easily modified to encompass other information based on business needs.

ACTION CHECKLIST: Security Assessment and Analysis

1. Identify a senior executive sponsor for the organization's overall security compliance program who acts as chief supporter, executive liaison, and "path smoother."

2. Designate a security compliance project leader.

3. Assemble a security assessment team.

    - Likely candidates in an organization would include information technology security staff, network staff, policy and planning staff, human resources, facilities management, financial staff, and business representatives.

4. Establish team structure, reporting relationships, meeting and report schedules.

5. Prepare an enterprise-wide Risk Assessment plan.

    - Break down the work and individual tasks
    - Estimate level and duration of effort
    - Calculate resource requirements
    - Assign responsibilities

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Develop timeline
- Determine deliverables
- Finalize budget

6. Develop baseline inventory of policies, procedures, practices, systems and forms.

   - Determine if/how the Y2K inventory can be applied
   - Identify "business associates" and review contracts
   - Identify existing security requirements the organization may have
   - Interview key staff to confirm or expand upon findings

7. Conduct technical, physical and administrative security review.

   - Overall architecture, including internal and external networks, and potential issues
   - Use of virus detection software, firewalls, other mechanisms
   - Applications and operating system security features
   - Communications security: e-mail, FAX usage, encryption, electronic signatures, Internet connections, etc.
   - Access points to networks and systems - internal and external
   - Data flow through systems and applications
   - Back-up systems and procedures
   - Websites and Intranets
   - User security practices such as logon/logoff, passwords, etc.
   - Support of users - internal and external
   - Workstation locations, policies and practices
   - Contingency and disaster planning
   - Physical security: locks, badges, pass codes, etc.
   - Incident reporting and follow-up

8. Identify gaps between the organization's current policies, procedures, systems and applications in all facilities, relative to the new security requirements.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Using the inventory, assess and document compliance levels, gaps and vulnerabilities against federal requirements and more stringent state provisions, where applicable

9. Perform a security risk analysis.

   - Use a methodology that is comprehensive but understandable and scalable, to facilitate risk mitigation
   - Include key managers in final analysis
   - Identify and evaluate risks in terms of
     1. value of assets,
     2. degree of exposure,
     3. likely consequences of incidents (including recovery costs, additional staff hours, loss of life, reputation or public trust, legal liability, etc.),
     4. probability and frequency of threat occurring,
     5. costs of alternative remediation measures, and
     6. organization's strategic objectives.
   - Rank priorities by comparing assets, vulnerabilities, threats and business goals
   - Risk mitigation does not pertain to prescribed measures

10. Perform impact analysis for minimum necessary access, uses and disclosures, considering:

    - Nature of disclosed information and importance to job functions and external relationships
    - Where information can be de-identified without interfering with needed functions
    - Costs and technologies for limiting information disclosure

11. Prepare final impact report, specifying details such as:

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Non-compliance
- Observed and potential risks
- Disparities between procedure, practice and/or culture, and new regulation requirements
- Opportunities for operational streamlining and cost savings
- Analysis of security risk management priorities and strategies
- Alternative security solutions and their costs
- Available resources
- Opportunities for security-related changes that will facilitate e-commerce goals
- Recommended security-related remediation and strategic measures[3]

It is important to note that management support and funding is crucial to the success of a security compliance project. If an organization were not fortunate to have obtained this approval first, the completed checklist matrix would also serve as a good tool to present to management for obtaining approval and funding. The checklist matrix will provide management with a good indication of the scope, size, cost and perhaps the complexity of the compliance project. In addition, the checklist matrix will illustrate the importance of implementing the security program across the enterprise.

MORE THAN ONE SET OF REGULATIONS

In some instances, organizations may be mandated to act in accordance with more than one set of security regulations. Basically, the security gap analysis process is the same for both sets. The added step is that you must compare the requirements of each regulation component to find those differences. Once the differences are found, determine which regulation is more stringent. The most stringent law will be the one to guide implementation. The differences obtained through this process should also be evaluated, prioritized, and incorporated into the compliance efforts.

RESOURCES AND TRAINING

Even though this may sound like a daunting project, there are many resources available to help with the process. For those choosing to outsource, there are IT security consulting firms specializing in providing services for assessment, gap analysis, and remediation.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

An organization should also consider utilizing the many security web resources that are available. To name a few, HIPAA's own website http://www.hipaadvisory.com provides a wealth of information and the National Institute of Standards and Technology (NIST) website http://www.nist.gov and the SANS Institute (CERT) website http://www.cert.org are also excellent sources. [10]

Software vendors are developing gap analysis tools for HIPAA readiness. However, not all software is created equal. Before purchasing a gap analysis tool, it is imperative to evaluate the organization's business needs to ensure using the product best suited to business needs. Web-based training is also available. HIPAA-On-line.com includes mediated chats for those who have purchased their online training packages.

For the health care industry, HIPAA conferences are also offering sessions on how to conduct a HIPAA Gap Analysis and Risk Assessment. The March 2002 HIPAA SUMMIT WEST II conference includes such topics as: How To's of Building a Security Matrix for Healthcare Organizations and Tracking Compliance, Developing a Two-Year Plan for Addressing HIPAA Data Security Requirements, and Conducting a Security Gap Analysis and Determining What To Do with the Results (Includes How to Establish a Baseline and Implement Monitoring). Since some of the health care industry is also impacted by the Gramm-Leach-Bliley Act, this conference provides focused coverage of its important security requirements. On a broader note, organizations like Computer Security Institute and the MIS Training Institute offer more general security courses with components addressing gap analysis and risk assessment.

MAINTENANCE OF SECURITY PROGRAM

The information security professional's job is not done once the security program is deemed to be in compliance. Continuous re-evaluation of the security program is essential. Virus creators, hackers and high tech thieves are becoming increasing sophisticated and an organization's computer defenses must continually grow to face the challenge. As new security laws or organizational standards are introduced, the process begins again. If an organization has developed and maintained a strong security program initially, the task will be more straightforward.

CONCLUSION

Complying with new security regulations does not have to be an overwhelming or rubber-stamp process. It can be a value-added exercise building knowledge of the organization's business needs and processes. From this effort, an organization can develop software and hardware inventories, vulnerability assessments, policies and procedures. Once the task is complete, an organization will know where the security strengths and weaknesses lie. This process may even reveal that the existing security program wasn't that bad after all.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

REFERENCES

1. Johnson, Amy Helen. "Gramm-Leach-Bliley: The Next Big Thing?" 25 June 2001 URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO61464,00.html (20 March 2002)

2. Costello, Sam. "Senator Pushes for Stronger Cybersecurity" 29 January 2002 URL: http://www.pcworld.com/news/article/0,aid,81763,00.asp (20 March 2002)
3. Phoenix Health Systems. "HIPAAlert – Vol. 2, No. 14 - 12/12/02" (12/12/01) URL: http://www.hipaadvisory.com/alert/vol2/number14.htm

4. Johnson, Amy Helen. "Closing the Security Gap" 25 June 2001 URL: http://www.itworld.com/Man/3887/CWD010627securitygap/ (20 March 2002)

5. Johnson, Amy Helen. "The Consultant Conundrum" 25 June 2001 URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO61473,00.html (20 March 2002)

6. Radcliff, Deborah. "Sizing Up Security Services" 27 November 2000 URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO54345,00.html (20 March 2002)
7. Dash, Julekha. "Beware of Predatory HIPAA Consultants" 7 May 2001 URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO60250.html (20 March 2002)
8. Koss, Shannah. "Getting Ready for HIPAA Security Requirements" *The 2000 Guide to Health Data Security* URL: http://houns54.clearlake.ibm.com/solutions/healthcare/helpub.nsf/detailcontacts/gettingready_1 (20 March 2002)
9. Johnson, Amy Helen. "Gap Analysis 101" 25 June 2001 URL: http://www.computerworld.com/storyba/0,4125,NAV47_STO61473,00.html (21 March 2002)
10. Phoenix Health Systems. "HIPAAnotes Vol. 1, No. 55" (12/15/01) URL: http://hipaadvisory.com/notes/vol1/dec01.htm (21 March 2002)

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.