Lab #3.2 Analyzing and Comparing GLBA and HIPAA

Introduction

Individuals and customers should normally expect companies and health providers to protect personal information. Custodians of private information should protect it as they would any other asset. Personal information has great market value both to other companies and would-be thieves. Because of this value, numerous examples exist of companies opting to share, sell, or inadequately safeguard their customers' personal information. The result has been two landmark pieces of legislation.

The purpose of the Gramm-Leach-Bliley Act (GLBA) and the Health Insurance Portability and Accountability Act (HIPAA) is to make organizations responsible and accountable for protecting customer privacy data and implementing security controls to mitigate risks, threats, and vulnerabilities of that data. Both of these laws impact their industries significantly.

In this lab, you will identify the similarities and differences of GLBA and HIPAA compliance laws, you will explain how the requirements of GLBA and HIPAA align with information systems security, you will identify privacy data elements for each, and you will describe security controls and countermeasures that support each.

Learning Objectives

Upon completing this lab, you will be able to:

- Identify the similarities between GLBA and HIPAA compliance laws.
- Identify the differences between GLBA and HIPAA compliance laws.
- Explain how GLBA and HIPAA requirements align with information systems security.
- Identify privacy data elements for both GLBA and HIPAA.
- Describe specific security controls and security countermeasures that support GLBA and HIPAA compliance.

Deliverables

Upon completion of this lab, you are required to provide the following deliverables to your instructor:

1. Lab Report file;
2. Lab Assessments file.

Hands-On Steps

▶Note:
This is a paper-based lab. To successfully complete the deliverables for this lab, you will need access to Microsoft® Word or another compatible word processor. For some labs, you may also need access to a graphics line drawing application, such as Visio or PowerPoint. Refer to the Preface of this manual for information on creating the lab deliverable files.

1. On your local computer, **create** the **lab deliverable files**.
2. **Review** the **Lab Assessment Worksheet**. You will find answers to these questions as you proceed through the lab steps.
3. On your local computer, **open** a new **Internet browser window**.
4. Using your favorite search engine, **search for information** on the **Gramm-Leach-Bliley Act.**
5. **Read** about this act.
6. Next, **research** the **privacy and security rules** for the Gramm-Leach-Bliley Act.
7. In your Lab Report file, **write** a thorough description of the Gramm-Leach-Bliley Act's basic components. Be sure to include the following topics:
   - Who co-sponsored the act?
   - Who is protected by the act?
   - Who is restricted by the act?
   - How are financial institutions defined?
   - What does the act allow?
   - How would you define the major parts of the privacy requirements: the Financial Privacy Rule, the Safeguards Rule, and the pretexting provisions? What do each of these spell out in the act? (**Write** three paragraphs on each of these.)
8. Using your favorite search engine, **research** the compliance law **HIPAA**.
9. In your Lab Report file, **write** a thorough description of HIPAA. Be sure to include the following topics in your discussion:
   - Which U.S. government agency acts as the legal enforcement entity for HIPAA compliance violations?
   - Who is protected by HIPAA?
   - Who must comply with HIPAA?
   - What is the relevance of health care plans, providers, and clearinghouses?

- How would you define the major parts of the Privacy Rule and the Security Rule? What do each of these spell out? (**Write** three paragraphs on each rule.)

10. In your Lab Report file, **describe** what the GLBA and HIPAA **privacy rules** have in common. Then, **discuss** how the two are different.

11. In your Lab Report file, **describe** what the GLBA and HIPAA **security rules** have in common. Then, **discuss** how the two are different.

Historical Differences Between GLBA and HIPAA

GLBA and HIPAA offer up historical similarities and differences. Both acts were drafted and made into law only a few years apart, with HIPAA in 1996 and GLBA in 1999. And both acts tackled gaps in information assurance and privacy, and are constructed similarly. However, HIPAA's Privacy Rule and Security Rule were published by the U.S. Department of Health and Human Services some four and seven years, respectively, after the act's passage. GLBA's Privacy Rule and Safeguards Rule were drafted alongside the original act.

Both acts target their particular industries with rules and control measures to protect information. However, each act's impact is limited based on where most of its industry is located. For instance, health care providers covered by HIPAA's mandate to protect information operate within the United States. By contrast, many large banks have locations and headquarters all over the globe, not just within the United States. But GLBA is enforceable only in the United States.

Yet another notable difference between the two acts is how dominant the issue of information confidentiality is to each act. HIPAA has two purposes: to help individuals retain health insurance and to help them control their personal data. GLBA's primary purpose is unrelated to information assurance altogether. Rather, GLBA was enacted to repeal many restrictions and regulations placed on banks from the Glass-Steagall Act of 1933. Once GLBA was in place, banks were free to consolidate and quickly grow without hindrance from any financial regulatory agency. In fact, popular opinion is that GLBA allowed banks to become "too big to fail," a phrase coined during the losing argument against GLBA in 1999. Consequently, history was made in 2007 with the U.S. financial crisis. But GLBA also ensured the banks would safeguard personal information.

12. In your Lab Report file, **discuss** how GLBA and HIPAA requirements align with information systems security.

13. In you Lab Report file, **list** two privacy data elements for GLBA and **list** two privacy data elements for HIPAA that are under compliance.

14. In your Lab Report file, **list** two security controls or security countermeasures for GLBA and **list** two security controls or security countermeasures for HIPAA that support compliance.

▶Note:
This completes the lab.

LAB #3.2 Analyzing and Comparing GLBA and HIPAA

Lab #3.2 - Assessment Worksheet

Analyzing and Comparing GLBA and HIPAA

Overview

In this lab, you identified the similarities and differences of GLBA and HIPAA compliance laws, you explained how the requirements of GLBA and HIPAA align with information systems security, you identified privacy data elements for each, and you described security controls and countermeasures that support each.

Lab Assessment Questions & Answers

1. Which U.S. government agency acts as the legal enforcement entity for businesses and organizations involved in commerce?
2. Which U.S. government agency acts as the legal enforcement entity regarding HIPAA compliance and HIPAA violations?
3. List three (3) similarities between GLBA and HIPAA.
4. List five (5) examples of privacy data elements for GLBA as defined in the Financial Privacy Rule.
5. List five (5) examples of privacy data elements for HIPAA as defined in the Privacy Rule.
6. List three (3) differences between GLBA and HIPAA.
7. How does GLBA's and HIPAA's privacy rule translate into information systems security controls and countermeasures?
8. What three areas does the GLBA Safeguards Rule encompass?
9. What is ePHI?
10. What three areas does the HIPAA Security Rule encompass for PHI?
11. Are organizations under GLBA and HIPAA required to mail and inform their customers in writing about their privacy tights?
12. When you go to your doctor's office, one of the forms the office asks you to fill in and sign is a

LAB #3.2 Analyzing and Comparing GLBA and HIPAA

HIPAA Release Form authorizing your doctor to share your medical records and privacy data with third parties, including health insurance companies. Is this an example of the HIPAA Privacy Rule or the HIPAA Security Rule?

13. Why is a Business Associate Agreement/Contract required between a HIPAA-covered entity and a downstream medical or service provider to that covered entity?

14. Like HIPAA, GLBA has both privacy and security rules. What are the official names of these rules in GLBA law?

15. True or false: GLBA encompasses insurance companies and stock brokerage firms.