CIS 481 – Intro to Information Security

IN-CLASS EXERCISE # 3 – Option C

Names of team members: Nick Cunningham, Shawn Nasr, Timothy Mahan, and Volodymyr Bestiyanets.

Logistics

A. Get into your regular team
B. Discuss and complete the assignment together. Don't just assign different problems to each teammate! That defeats the purpose of team-based learning.
C. Choose a recorder to prepare the final copy to submit to instructor in Blackboard.

Problem 1
The Health Insurance Portability and Accountability Act (HIPAA) was designed to help keep the protected health information (PHI) of consumers private and secure. The HITECH Act, passed in 2009, broadened the PHI protections afforded by HIPAA and enforced data breach notification requirements on covered entities and business associates. The Omnibus Regulations further amended the protections of HIPAA and HITECH in 2013.

Resources for HIPAA are numerous online. A good collection of articles can be found at:

https://datica.com/academy/ (a vendor site, so some pushing of their product is to be expected).

Follow the article sequence here and then answer the following:

HIPAA 101
What is PHI?
The HIPAA Privacy Rule
The HIPAA Security Rule
HIPAA Risk Assessment and Management
HIPAA and Encryption
HIPAA and Data Breaches

1. What/who are *covered entities*? *Business associates*? (5 pts.)

Covered entities include health systems, hospitals, health care providers, insurers of health care, and health care clearinghouses which change and process health insurance information for payers and providers. Business associates are entities such as individuals and organizations, including subcontractors, that provide services and/or technology to covered entities. These services involve the access, transmission, and storing of Protected Health Information (PHI). Any entity that handles the PHI of a covered entity is a business associate. Examples of business associates include accountants, third -party vendors of software, lawyers, web hosts, storage services, data processing firms, third party administrators, and various other services/technology.

2. Describe two methods of de-identifying PHI. Do you think the 18 elements considered to uniquely identify an individual are sufficient? Why or why not? (5 pts.)

De-identifying an individual is the process of masking unique information to that individual in order to protect their privacy. An example would be if a patient was to take place in an experimental Aids treatment. That person would not want it known that they carried such a virus and were undergoing treatment except only by medical professionals. Pseudonymization is the process of replacing unique identifiers such as names with a medical ID known only for specific purposes. Instead of Bob, the individual could be patient X473. K-anonymization attributes common identifiers to an individual instead of unique information. Bob could be referred to as middle-aged, white, and male instead of his given birth name. I believe that some of the 18 elements are sufficient, when others are not. To be unique the identifying elements need to be unique to that individual, while some are too generalized, and others too easily fabricated. A social security number is very unique while dates, fax numbers, and geographic locations by themselves don't stand up on their own.

3. Describe the three major categories of safeguards in the Security Rule. Which is the largest area? (8 pts.)

The three major categories of safeguards in the Security Rule are the Administrative, Physical, and Technical. The largest by far is the Administrative, which makes up about 50% of the rule. The Administrative category mainly deals with the policies and processes around sensitive data, as well as the risk-assessment that goes along with securing the data from all aspects. Here, we layout our architecture, find risks, and mitigate risks. Next is the Physical, which deals primarily in the physical security of the medium used to house, encrypt, and manipulate the data. This includes ensuring that no unauthorized personnel (such as the cleaning crew) have access to areas where the sensitive information is stored. Finally, we have the Technical category. The technical category includes things like encryption during transmission, encryption while the data is at rest, and logging all activity that surrounds the sensitive data you're protecting. This logging includes any data manipulation, transmission, and API calls made. You pretty much just log who accessed what at a specific time for any and all transactions.

4. What should be the first step in the process of securing ePHI? Explain your reasons. (7 pts.)

The first and one of the most vital steps in the process of securing a ePHI, or any digital information containing personally sensitive information, is to ensure that the information is properly encrypted. Implementing the technical safeguards is necessary to establish the foundation of the security of the information on which the rest of the safeguards then build upon. This foundation assures that the information can still maintain its confidentiality even if that information is compromised by an individual or entity that is not authorized to have access to the sensitive personal and medical information contained within the ePHI.