Final Project

Ahmad Shekib Nawabi, Allyson Bryne, Athena Bryant, and Travis Vance

MCSOL, University of San Diego

CSOL-510-04-SP22: Applied Cryptography

Instructor: Thomas Plunkett

04/11/2022

Table of Contents

1. **Executive Summary……4**
2. **Section 1……..….5**
   - **HIPAA Regulations**
3. **Section 2…….……..7**
   - **Security Goals of the Company and Security Policies**
4. **Section 3…….……9**
   - **Major Cyber Threats Facing the Company**
5. **Section 4 ……10**
   - **Cryptographic Controls Proposed**
6. **Section 5 ……12**
   - **Risks vs. Cost Tradeoffs**
7. **Conclusion……13**
8. **References……...……...15**

Table of Glossary

Cryptography	**Security controls that shield information from prying eyes.**
Phishing Attack	**The fraudulent practice of sending emails purporting to be from reputable companies to induce individuals to reveal personal information, such as passwords and credit card numbers.**
Malware	**Software is designed to disrupt, damage, or gain unauthorized access to a computer system.**
Ransomware	**is malicious software designed to block access to a computer system until a sum of money is paid.**

Executive Summary

IT security at X health insurance company is concerned with the increase of worldwide ePHi cyber-attacks. Malware attacks, phishing attacks, insider threats, crypto mining, crypto-jacking Malware, DDoS (Distributed Denial of Service), Botnet attacks, supply chain attacks, ransomware, advanced Malware, etc., are threats cybersecurity professionals need to take into account. (Cysiv, 2019) This document proposes securities and controls by HIPAA (Health Insurance Portability and Accountability Act) 45 CFR 164.308.

"In a 2021 survey of 597 health delivery organizations (HDOs), 42% had faced two ransomware attacks in the past few years. Over a third (36%) attributed those ransomware incidents to a third party." (Bisson, 2021)

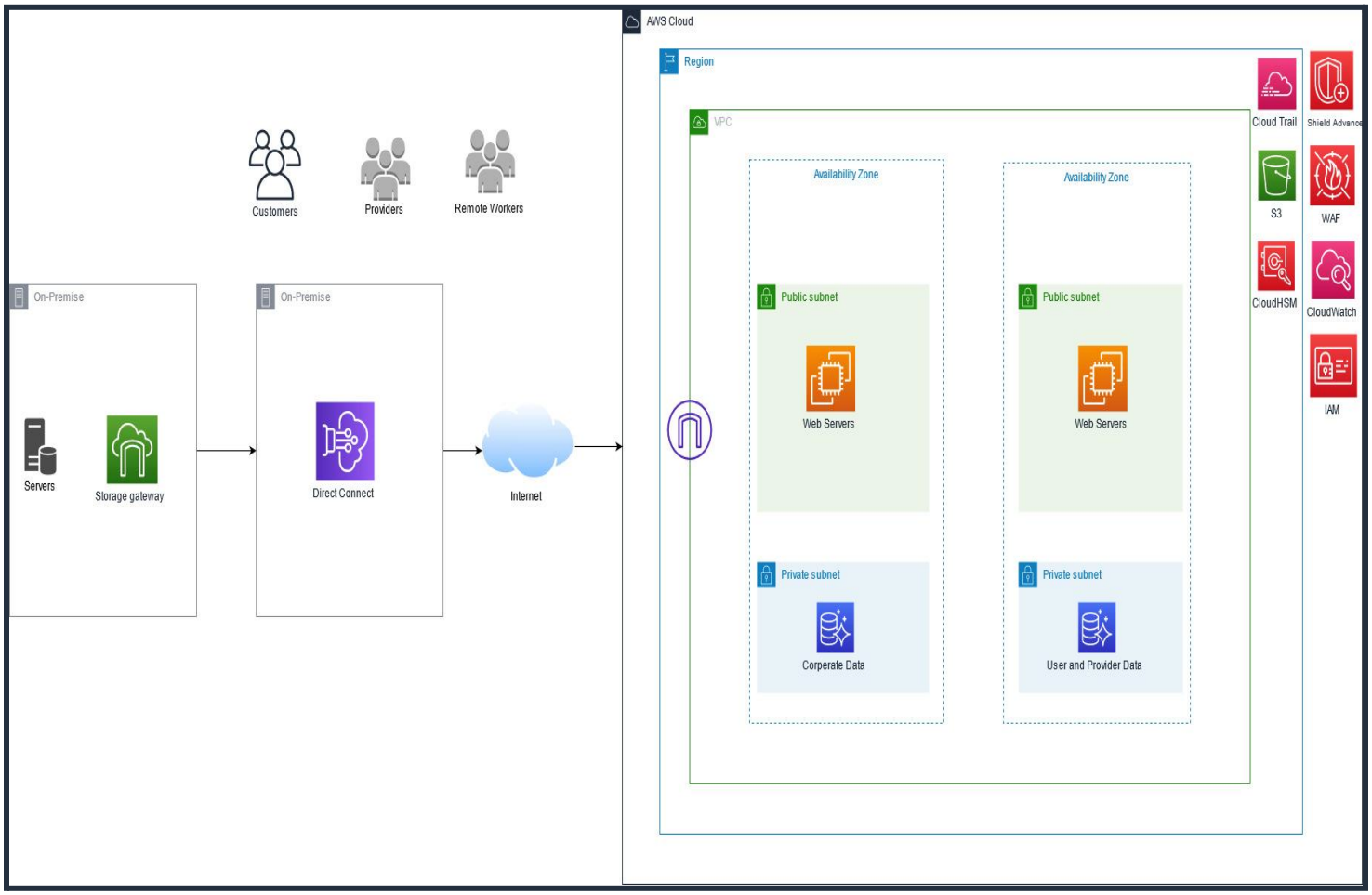
The X health insurance company IT security team studied recent threat actors. This document surfaces the study's results, industry regulations, the draft of required policies, and security controls to implement based on guidelines.

Also, the paper recommends actions that will improve the security posture.

Introduction,

The purpose of this document is to propose HIPAA-compliant security controls based on the company's network architecture. HIPAA rules and regulations cover three pillars: HIPAA privacy rules, security rules, and breach notifications. HIPAA rules and regulations document how to obtain HIPAA compliance. HIPAA violations could result in fines of up to $25K and loss the customer's trust. The key to protecting consumer information, precisely personal health information (PHI) data, is to understand the associated rules and regulations, conduct a risk analysis, and implement security controls identified through the assessment.

Architecture Health Organization:



Section 1: HIPAA Regulations

45 CFR Part 164.308

AWS cloud services will provide the perfect solution for a cloud computing environment subjected to strict governance, such as this scenario. AWS is the ideal way to build applications that store, process, and transmit sensitive health-related information, consistent with your privacy and security obligations under frameworks such as the US Health Insurance Portability and

Accountability Act (HIPAA) or The Federal Risk and Authorization Management Program (FedRAMP) as well NIST compliant.

Components

Customers: Customers will have access to hosted resources only in the public domain(s)/subnets–as depicted in the diagram above, both web servers will be accessible to customers.

Providers/Remote Workers: With Identity Access Management (IAM), you can manage AWS permissions for workforce users and workloads. For workforce users, it is recommended that you use AWS Single Sign-On (AWS SSO) to control access to AWS accounts and permissions within those accounts. AWS SSO makes provisioning and managing IAM roles and policies more accessible across your AWS organization. Use IAM roles and policies for workload permissions, and grant only the required access for your workloads.

Off-Site Backup: The offsite backup storage will be provided via the AWS storage gateway. Storage Gateway enables you to reduce your on-premises storage footprint and associated costs by leveraging AWS storage services. All data transferred between the gateway appliance and AWS storage is encrypted using SSL–AWS Storage Gateway is HIPAA compliant.

Firewalls: All firewall configurations are supported by AWS WAF. This will simplify managing individual firewalls throughout the network in one central location.

Web Servers: Many ways secure servers within the AWS environment.

- **Least Access**: Restrict server access from both the network and on the instance
- **Least Privilege:** Define the minimum set of privileges each server needs to perform its function.
- **Configuration Management:** Create a baseline server configuration and track each server as a configuration item. Ensure each server is configured to generate and securely store appropriate log and audit data through the Cloud Watch logging service.

- **Change Management:** Create processes to control changes to server configuration baselines.
- **Audit Logs:** Audit access and all changes to EC2 instances to verify server integrity to ensure only authorized changes are made.

VPN: All VPN needs are hosted via AWS Direct Connect, and data is delivered through a private network connection between your facilities and AWS. In many circumstances, private network connections can reduce costs, increase bandwidth, and provide a more consistent network experience than internet-based connections.

User and Provider/ Corporate Data - AWS cloud provides vast database solutions. In this scenario, the selected choice of Amazon Aurora is designed to offer 99.99% availability, replicating six copies of your data across 3 Availability Zones and backing up your data continuously to Amazon S3. Amazon Aurora provides multiple levels of security for your database. These include network isolation using AWS VPC, encryption at rest using keys you create and control through AWS Key Management Service, and data encryption in transit using SSL.

CloudHSM: Our cryptography solution - Our Solution leverages AWS CloudHSM service. This will help meet contractual and regulatory compliance requirements for data security by using dedicated Hardware Security Module (HSM) instances within the AWS cloud. CloudHSM complements existing data protection solutions and allows the protection of your encryption keys within HSMs designed and validated to government standards for secure key management. CloudHSM will enable you to securely generate, store, and manage cryptographic keys used for data encryption.

Section 2: Security Goals and Security Policies

Security Goals

1. Ensure the confidentiality, integrity, and availability of PHI they create, receive, maintain or transmit;

2. Identify and protect the security and integrity of information against reasonably anticipated threats;

3. Protect against reasonably expected, impermissible uses or disclosures;
4. Ensure workforce compliance with security goals and security policies.

Security Policies:

1. Security Management Process
2. Assign Security Responsibility
3. Workforce Security
4. Information Access Management
5. Security and Awareness Training
1. Security Incident Procedures
2. Contingency Plan
3. Evaluation
4. Third-Party Risk Management

Section 3: Major Cyber Threats facing the Company

1. Data Stealing Threats focus on monetizing personally identifiable data (PII) and protected health information (PHI). The bad actors target valuable research and patient health records for intelligence gathering.

2. Disruptive and Destructive Threats, such as ransomware, can disrupt healthcare networks, impacting critical biomedical devices and systems. (*Cysiv*, 2019)

Attack Methods

1. **Insider Threats:** Malicious threats that are internal to an organization. For example, disgruntled or rogue employees.
2. **Spam and Phishing Attacks:** Attackers disguise themselves as known, trustworthy organizations or people to obtain information.
3. **Ransomware and Advance Malware Attacks (e.g., Trojan, Spyware):** Malicious software (Malware) is designed by an attacker to damage and destroy the target's computers and computer systems.
4. **DDoS and Botnet Attacks:** Distributed denial-of-service (DDoS) is a targeted attack that floods a network or server until the "service" shuts down.
5. **Supply Chain Attacks:** Supply Chain attacks infiltrate companies via third-party software and vendors. The intent is to access the target company using a trusted entity.
6. **Crypto-Mining, Crypto-Jacking Malware:** Crypto-jacking occurs when a lousy actor hacks into a device (i.e., computers, phones, servers, tablets) for the sole purpose of using it to mine cryptocurrency.
7. **Medical Device Attacks:** Malware, ransomware, and other attacks targeted at medical devices inside and outside health organizations.
8. **3rd-Party Attacks:** Similar to supply chain attacks, vendors abuse access to an organization to obtain physical and logical access to data.

Section 4: Cryptographic Controls Proposed

Link in the references by Lau, V. base it off of network architecture diagram in Module 7.

Section 5: Risks vs. Tradeoffs

"Data breaches can significantly impact the healthcare organization attacked and the individual victims. Healthcare and Public Health Sector (HPH) sector entities face the cost of recovery, lawsuits, and the public relations ramifications, including loss of customers/patients. Individuals can suffer financial penalties of various sorts and the embarrassment of having personal information leaked." (Health Sector Cybersecurity Coordination Center, 2019)

The X health insurance company could be subjected to increased cyber attack risk based on their industry. The first action is determining the organization's priorities and conducting a risk analysis before implementing security controls. "A trade-off between security and privacy can be broken down into two trades: the trade-off between security and money and the trade-off between privacy and money." (Giordani, 2021)

Organizations are known to focus on short-term gains rather than long-term goals. Often, the short-term gains include making trade-offs that push out privacy and security work. Security can hinder a company's ability to move fast, but there are cyber threats that could do more harm—for example, looking at the Target breach. A new vendor could become a viable threat. The company's security team must vet the new vendor, ensuring that the vendor complies with mandatory regulations before engaging in business activities. The time onboard could require more time than the allocated by the business. However, the security team must confirm that the vendor's remit aligns with the business need, document the required data, how/when the data is transferred and stored and implements security controls. The upfront inconvenience can be worth it in the long run.

Another example is when our organization stores sensitive data, such as in the applications and Back-Up Network Attached Storage (NAS) shown in the network diagram. Implementing encryption on these devices and databases per regulations and laws is required. However, with encryption, there have been arguments that it could hurt processing speeds as data needs to be encrypted before it can be read.

As mentioned above, outsourcing services such as AWS for cloud storage and hosting can help cut costs and management of hardware and software.

Cybercrime damages are increasing year-over-year (YoY). McAfee's annual report detailed public and private cybercrime physical and financial losses. For 2020, McAfee states that the business impact of cybercrime costs more than one trillion dollars. The cost of cybercrime will likely continue to increase since we've noticed a dramatic increase since 2018. (Guim, 2021)

On May 6, 2021, the Colonial Pipeline was hacked, and the company reportedly paid a $5MM ransom. In May of 2021, JBS, a Brazilian meatpacking company, became a ransomware attack victim. JBS' paid the $4.4MM ransom, but the loss of revenue could've been even higher than the ransom. Hackers have started to make the healthcare industry a top priority. The healthcare industry is attractive because of 1) the richness of the stored data (e.g., PII and PHI); 2) security controls with minimal investment; and 3) disparate systems that are cobbled together to connect. In recent years, US healthcare breach costs have increased. One study determined that the price of a single stolen healthcare record increased from $363 to $380 from 2015 to 2017. (Landi,2022)

Conclusion

Our company is in a highly targeted industry by bad actors. These regulations and laws are being implemented to force companies in this field to build up their cyber defenses and ensure layers of protection. The document has outlined the HIPPA controls needed to be compliant. As stated, HIPAA violations could result in fines of up to $25K and customer trust loss. The key to protecting consumer information, specifically personal health information (PHI) data, is to understand the associated rules and regulations, conduct a risk analysis, and implement security controls identified through the assessment.

References

Bisson, D. (2021, November 24). Hospital Ransomware Attacks Go Beyond Health Care Data. Retrieved from https://securityintelligence.com/articles/hospital-ransomware-health-care-data/

Cysiv, LLC. (2019, November 26). Threat Report: Threats & Threat Actors Targeting Healthcare. Retrieved from https://cdn2.hubspot.net/hubfs/6893765/AMER%20Content%20Downloads%20(PDFs)/Reports/Cysiv%20Threat%20Report%20-%20Healthcare%20(11-26-19)%20FINAL.pdf

Hipaaguide.net. (2021, October 14). What is 45 CFR 164.308? Retrieved from https://www.hipaaguide.net/what-is-45-cfr-164-308/

Lau, V. (n.d.). HIPAA Encryption: Requirements, Best Practices & Software. Retrieved from https://www.kiteworks.com/hipaa-compliance/hipaa-encryption/

Giordani, J. (2021, June 3). *Council post: How to balance trade-offs between security and privacy in it*. Forbes. Retrieved April 14, 2022, from https://www.forbes.com/sites/forbestechcouncil/2021/06/03/how-to-balance-trade-offs-between-security-and-privacy-in-it/?sh=26d27fef66a6

Guim, T. (2021, August 10). *Cost of cyber attacks vs. the cost of cyber security in 2021*. PCH Technologies. Retrieved April 14, 2022, from https://pchtechnologies.com/cost-of-cyber-attacks-vs-cost-of-cyber-security-in-2021/

Landi, H. (2022, February 1). *Healthcare data breaches hit an all-time high in 2021, impacting 45M people*. Fierce Healthcare. Retrieved April 14, 2022, from https://www.fiercehealthcare.com/health-tech/healthcare-data-breaches-hit-all-time-high-2021-impacting-45m-people