Project Proposal

SRA 311

October 11, 2019

Kira Kuzmenchuk

Ryan Fletcher

David Ramadhani

Edward Park

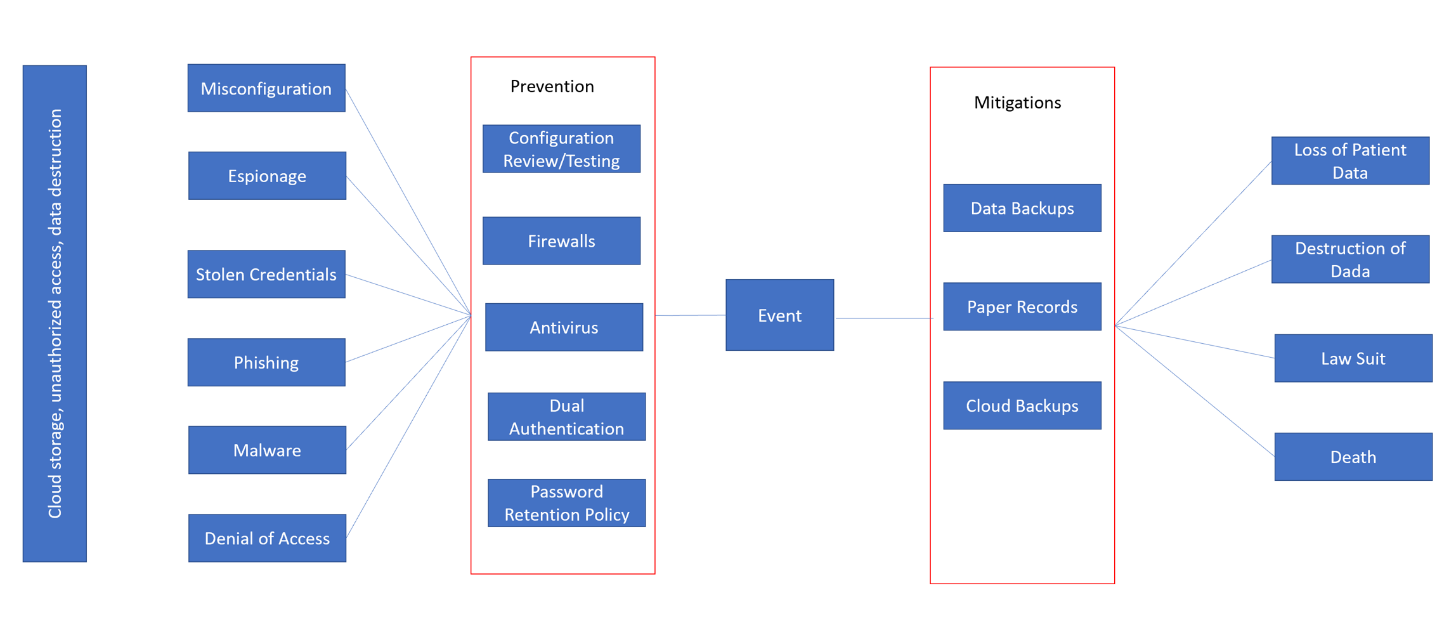
1. Project Link
   1. Github
      1. The following repository was established to track living documents and files. This repository also provides a central point to view documents while auditing changes
      2. Kira Kuzmenchuk - <https://github.com/insyder5000/SRA-311-Risk_Project>
2. Executive Summary

This document is to discuss the risks associated with handling electronic patient records. The lower cost of operations is a big use case behind moving certain operations or processes to the cloud, but with that lower costs also introduces more risk. This document will serve as an analysis of the threats, likelihood of attacks, and stakeholders involved with this kind of project. The question we must ask is “How do we protect our customers confidential information stored electronically?” A health care organization has very strict regulations on protecting patient records and in a world as interconnected and the demand to have information easily accessible on a number of devices protecting that data is a critical challenge. We will be utilizing the National Institute of Standards and Technology (NIST) framework document 800-53 (https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.02192014.pdf) to outline the steps in identifying risks involved with these records and will set up controls for each of those risks. Our project can bring a substantial benefit in highlighting the current shortcomings in defense model and can potentially reduce risk surface. Per the HIPPA Journal the average data breach in the Health Care industry consists of about 25,500 records and costs about $430 dollars per record. This can come out to be about 3.92 Million dollars per incident. (<https://www.hipaajournal.com/2019-cost-of-a-data-breach-study-healthcare-data-breach-costs/>) Depending on the potential number of risks and their likelihood the cost could increase exponentially.

1. Background Information of the Organization
   1. Sector: Healthcare
   2. Leadership Team:
      1. President & CEO: Clint Matthews
      2. Executive Vice President and Chief Operating Officer: Therese Sucher
      3. Executive Vice President, Strategy and Business Development: Daniel Ahern
      4. Executive Vice President and Chief Financial Officer: Gary Conner
      5. Executive Vice President and Chief Medical Officer: Dr. Greg Sorensen
      6. Senior Vice President and Chief Nursing Officer: Mary Agnew
      7. Vice President, Chief Compliance Officer: Shane Campbel
      8. Legal Counsel: Joanne Judge
   3. Employees: 11,000+
   4. Physicians: 2000+
   5. Locations: 65 across Eastern Pennsylvania
2. Stakeholder Analysis

|  |  |  |
| --- | --- | --- |
| Stakeholder | Description | Importance |
| Patient | A person who is under medical care or treatment or whose records are kept within a healthcare institution | 4 |
| Employees | A person who is an employee of a healthcare institution | 3 |
| Insurance Companies | Company that pays for patient care and treatments | 2 |
| Government | Administration that regulates healthcare policies and privacy | 2 |
| Board of Directors | Board that consists of people who oversee institution changes and management | 2 |

1. Project Scope Statements
   1. Major Business Procedures
      * Reporting - Business reports are a type of assignment in which you analyze a situation and apply business theories to produce a range of suggestions for improvement.
      * Production - This is the area that functions the business and turns inputs (raw materials) into finished products or outputs through a series of production processes.
      * Operations - The obligations of the Operation department can change from business to business. In any case, its objectives, including that of the managers who run them, are usually equivalent. Principally, it is the one liable for administering, planning and controlling the procedure of production. They can likewise overhaul business tasks if important.
      * Customer Service - Customer Service Representatives are the principal line of contact with the general population for some organizations. With that being the case, one of the essential duties of this division is to build up and concrete the relationship of your business to the general public. A good Customer service Office will have the option to make, keep up, and hold the relationship of the business to its clients.
   2. The annual report is related to the reporting. It provides the information such as General description of the industry or industries in which the company is involved. Audited statements of income, financial position, cash flow, and notes to the statements providing details for various line items. The production is also important because it works to improve the efficiency of the company. During the operations of the company the workers must perform tasks that will provide service to the customer's needs. Customer Service provides the customers what they need when an issue has been brought up and needs to be taken care of at hand.
2. Preliminary Risk Analysis
   1. Hazardous Events
      1. Forgetting password to login
      2. Errors within software design
      3. Administrating wrong doses based off previous medical records
      4. Confusion between medical records online and on paper
      5. Data can be duplicated/deleted
      6. Duplication can leads to multiple mistakes
      7. Cloud Storage
      8. Unauthorized Access
      9. Privacy Breaches
      10. Data Destruction
      11. Doctor-Patient relationship becomes impersonal
   2. Triggers
      1. Misconfiguration
      2. Espionage
      3. Stolen Credentials
      4. Phishing
      5. Malware
      6. Denial of Access
   3. Prevention Barriers
      1. Configuration review/testing
      2. Firewalls
      3. Antivirus
      4. Dual Authentication
      5. Password Retention Policy
   4. Mitigation Barriers
      1. Data Backup
      2. Paper Records
      3. Cyber Insurance
   5. Consequence
      1. Loss of patient data
      2. Destruction of data
      3. Lawsuit
      4. Death
      5. Loss of Reputation



1. Data Collection and Analysis

We are focusing on data breaches of electronic patient data for this project. I am unsure if we will be able to get any specific data from Tower Health but there are national databases for statistical data from the healthcare division.

Types of data we may need are:

* Quantitative data on how many data breaches have occurred
* Quantitative/Qualitative data on how the breach has affected Tower Health or other healthcare organizations
* Quantitative data on the down time an institution experienced after the breach
* Qualitative data on the preventive and reactive measures an institution has taken into consideration against breaches

A few places we are likely to obtain the data are governmental healthcare databases, FDA statistics, and other medical databases. We should be able to find many real-world specific use cases via the Verizon Data Breach Incident Report (DBIR) and the Symantec Internet Threat Security Report (ITSR) as well. We can then use this data to form a test plan and run simulations to find the likelihood and probability of different threats. We may be able to use simulations to gauge the number of records breached, which can then be used to estimate the potential impact of each incident.

The places we are mostly like to find issues getting data is data specific to Tower Health as some of that data may be restricted to internal personnel only.

|  |  |  |
| --- | --- | --- |
| Data Type | Simulation | Difficulty |
| # of data breaches | Poisson model | 3 |
| Effect of data breach | unknown | 4 |
| Down time post breach | unknown | 3 |
| Preventive measures | unknown | 2 |
| Reactive measures | unknown | 2 |

1. Development Plan

|  |  |  |
| --- | --- | --- |
| Deliverable | Due Date | Responsible |
| Proposal | 10/11/19 | See below |
| Background information | 10/10/19 | Kira |
| Executive Summary | 10/10/19 | Ryan |
| Stakeholder analysis | 10/10/19 | David |
| Project scope | 10/10/19 | David |
| Preliminary risk analysis | 10/10/19 | Edward |
| Data collection & analysis | 10/10/19 | Ryan |
| Development plan | 10/10/19 | Kira |
| Review | 10/10/19 | Edward |
|  |  |  |
| Presentation | 12/6/19 | See below |
| Background information | 11/22/19 | Kira |
| Executive Summary | 11/22/19 | Ryan |
| Stakeholder analysis | 11/22/19 | David |
| Project scope | 11/22/19 | David |
| Preliminary risk analysis | 11/22/19 | Edward |
| Data collection & analysis | 11/22/19 | Ryan |
| Development plan | 11/22/19 | Kira |
| Review | 11/22/19 | Edward |
|  |  |  |
| Paper | 12/6/19 | See below |
| Background information | 11/22/19 | Kira |
| Executive Summary | 11/22/19 | Ryan |
| Stakeholder analysis | 11/22/19 | David |
| Project scope | 11/22/19 | David |
| Preliminary risk analysis | 11/22/19 | Edward |
| Data collection & analysis | 11/22/19 | Ryan |
| Development plan | 11/22/19 | Kira |
| Review | 11/22/19 | Edward |