RISK MANAGEMENT: ELECTRONIC PATIENT RECORDS WITHIN TOWER HEALTH

Kira Kuzmenchuk

Ryan Fletcher

Edward Park

David Ramadhani

Table of Contents

Contents

1. Project Link

As a team, we used Microsoft Teams and Github for our working documents to allow for group work on living documents.
Our Github link is: https://github.com/insyder5000/SRA-311-Risk_Project

2. Executive Summary

This document is will discuss the risk analysis conducted against the risks associated with handling electronic patient records within Tower Health, a healthcare organization. Tower Health has made a commitment to provide high-quality, cost-effective care in the communities they serve. 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.

As a healthcare organization, Tower Health has major assets with their organization. Hardware assets within the organization include servers, medical devices, and other medical equipment used for the care of their patients. Tower Health's major environmental resource is the physical buildings in which Tower Health operates. The environmental factors including weather externally and cleanliness of the interior is important aspect to the asset. Liveware is a major aspect of Tower Health since they are a healthcare organization. The patients, physicians, nurses, and all other staff make up the live ware assets of Tower Health. Finally, Tower Health has major software assets which include medical and person information of over 2.5 million patients. This is the asset we will be concentrating on within this risk analysis.

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 costs approximately $430 dollars per record. This can come out to be about 3.92 Million dollars per incident (1). Depending on the potential number of risks and their likelihood the cost could increase exponentially. Constraints of this analysis include our access to information and legal compliance.

3. Background Information of the Organization

3.1 Overview

A. Organization: Tower Health
B. Sector: Healthcare
C. Leadership Team:
   a. President & CEO: Clint Matthews
   b. Executive VP and Chief Operating Officer: Therese Sucher
   c. Executive VP, Strategy & Business Development: Daniel Ahern
   d. Executive VP & Chief Financial Officer: Gary Conner

   e. Executive VP & Chief Medical Officer: Dr. Greg Sorensen
   f. Senior VP & Chief Nursing Officer: Mary Agnew
   g. Vice President, Chief Compliance Officer: Shane Campbel
   h. Legal Counsel: Joanne Judge

D. Employees: 11,000+
E. Physicians: 2,000+
F. Locations: 65 across Eastern Pennsylvania

3.2 Missions

Tower Health's main mission is to provide compassionate, accessible, high quality, cost effective healthcare to the community, to promote health; to educate healthcare professionals; and to participate in appropriate research.

Tower health achieves its goal of providing compassionate, high-quality healthcare by having the best staff on hand, great customer service (bedside manner, patient management) and by providing patients access to state-of-the-art treatment.

Tower health achieves its goal of providing accessible, cost-effective healthcare by having the 65 locations to allow easy access to a healthcare facility and working with the government and additional stakeholders to try and keep costs down for patients.

Tower health achieves its goal of promoting health though its advertisements of treatment programs, addiction management, and primary care.

Tower health achieves its goal of educate healthcare professionals by running a nursing school in reading and providing a top residency program for new doctors.

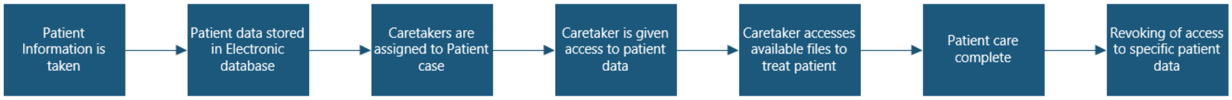
Tower health achieves its goal of participating in appropriate clinical research by having cancer research centers, running clinical trials and working with the medical community to learn more about what treatments need to be discovered.

3.3 Business Functions

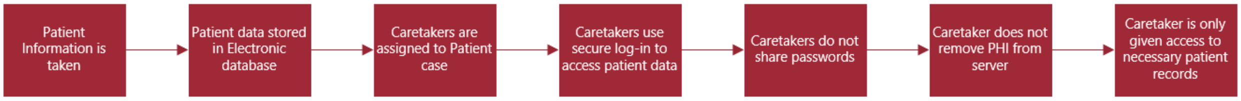
Healthcare institutions have many essential business functions to keep running including:

- Patient Care (Customer Service) – care of patient
- Finance – income to support function of hospital
- Research & Development
- Information Technology (Focus of our analysis)
  - Ensure Patients and Caretakers have access to available patient data
  - Protect patient data protected
  - Physical integrity of systems
- Operations – daily operations of Healthcare Institution

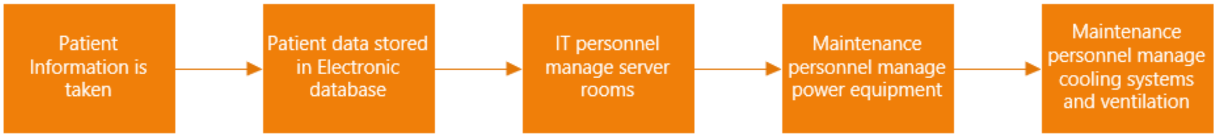
The three business functions we will be focusing on within our analysis is ensuring patient data is available, ensuring integrity of patient data and protection against data theft and protection of physical systems. The flow charts for each business function are shown below.


Patient Information is taken
Patient data stored in Electronic database
Caretakers are assigned to Patient case
Caretaker is given access to patient data
Caretaker accesses available files to treat patient
Patient care complete
Revoking of access to specific patient data

Ensuring patients and caretakers have access to available patient data is a crucial function in a healthcare institution. Without access to patient information, caretakers including doctors and nurses cannot properly take care of the patient. When a patient's information is entered into the system, it is stored in an electronic database. Caretakers are assigned to a specific patient's case and that caretaker is given access to the patient's records. Once treatment is complete or a patient's care is transferred to another caretaker, the patient access should be revoked from the previous caretaker.


Patient Information is taken
Patient data stored in Electronic database
Caretakers are assigned to Patient case
Caretakers use secure log-in to access patient data
Caretakers do not share passwords
Caretaker does not remove PHI from server
Caretaker is only given access to necessary patient records

Ensuring patient data is protected from theft or manipulation is another crucial business function a healthcare institution must uphold. The diagram above demonstrates how caretakers help prevent unauthorized access to patient data. Using secure log-in, not sharing passwords, preventing removal of PHI from the server and only giving access to necessary personnel are ways that individuals can help protect PHI.


Patient Information is taken
Patient data stored in Electronic database
IT personnel manage server rooms
Maintenance personnel manage power equipment
Maintenance personnel manage cooling systems and ventilation

Protection of the physical systems where EHR data is stored is necessary to try and prevent the loss or damage of electronic data. Physical security measures need to be put in place to mitigate the risk of physical damage occurring to the data housing systems and loss or destruction of data. The management of physical system updates and replacement of old hardware aid in the continuing work of the institution. Physical safety mechanism including automatic fire-retardant and use of antistatic clothing also protect the physical systems from being compromised.

All three business functions are not only dependent on individuals work but on the system that information is stored on and the management of those systems. Keeping healthcare systems up-to-date and ensuring correct procedures and network configuration help protect patient data.

4. Stakeholder Analysis

4.1 Stakeholder Analysis

Stakeholder	Description	Type	Importance
Patient	A person who is under medical care or treatment or whose records are kept within a healthcare institution	Definitive	High

Employees	A person who is an employee of a healthcare institution	Dependent	Medium
Insurance Companies	Company that pays for patient care and treatments	Dangerous	Medium
Government	Administration that regulates healthcare policies and privacy	Dangerous	Medium
Board of Directors	Board that consists of people who oversee institution changes and management	Dominant	Medium

4.2 Impact on Stakeholder's Interests

The impact of our project can greatly affect all stakeholders within this organization. Starting at the top, the government's interest in healthcare management will be affected as our analysis can demonstrate the weak points within a large healthcare organization.

The Board of Director's interest is in the changes and management within the Tower Health organization. The results of our analysis can directly affect the changes they chose to implement to better protect the organization.

Employees' interest is in the care of the patients and individuals that come in and out of the doors of each one of the Tower Health locations. The results of our analysis could result in better security training for the employees. When the employees know how to better protect their patient's information, it increases the security their patients feel which increases their view on their care.

Patients main interest is in getting the care they need while being cared for within the Healthcare organization. Our analysis, along with the implementation of changes from the Board of Directors can result in a greater peace of mind that their information is safe within the organization.

Insurance companies have interest paying for patient care, therefore they interest are the least affected by our analysis. The protection of insurance information is the main affected interest from our analysis.

5. Project Scope Statements

We have chosen to focus on these functions because they are three of the most crucial functions to the survivability of a healthcare institution. While patient records did not used to depend on technology, 99% of hospitals used electronic health records (HER) as of 2017 (2). All three business functions support Tower Health's mission statement to provide high-quality, accessible, cost-effective healthcare. The addition of technology has increase in the quality of healthcare provided to patients. Electronic health record management also supports accessible, cost-effective healthcare as it is cheaper to manage and access online health records.

5.1 Business Function Assets

Seeing as all three of our business functions relate to patient electronic health records, they all have the similar assets.

Data Accessibly/Available	
Data	Patient data
Hardware/Machinery	PACS systems, Healthcare computers, servers
Software Systems	Patient Management system, access management lists
Employees	Healthcare providers and IT administrators
Facilities	Healthcare office, hospitals, urgent cares

Data Integrity & Protection from Theft	
Data	Patient data
Hardware/Machinery	PACS systems, Healthcare computers
Software Systems	Patient Management system, firewalls, internal network architecture
Employees	IT administrators
Facilities	Healthcare office, hospitals, urgent cares

Physical System Protection	
Data	Patient data
Hardware/Machinery	Servers, laptops, desktops
Software Systems	Patient Management system, system management software
Employees	IT administrators
Facilities	Healthcare office, hospitals, urgent cares

5.2 Potential Security Accidents

Data Accessible/Availabile		
Accident	**Category**	**Will we cover?**
Access provided to incorrect person	2	No
Power outage	1	Yes
System Outage	2	Yes
Loss Internet	1	Yes
Network Outage	1	Yes
Provided locked out of individual patient record	2	No

Data Integrity & Protection from Theft		
Accident	**Category**	**Will we cover?**
Hack	3	
Employee theft of individual records	3	
Encryption failure	2	
Network Infiltration due to firewall failure	2	

Physical System Protection		
Accident	**Category**	**Will we cover?**
Fire	3	Yes
Natural Disaster	2	Yes
Intentional physical destruction of hardware	2	No
Data Center Power Failure	2	Yes – related to Natural Disaster
IT Human Errors	2	Yss

6. Risk Analysis

6.1 Hazardous Events and Bow-Tie Diagrams

6.1.1 Data Accessible/Available

Our first hazardous event that can affect the accessibility of available patient data is network outage. A network outage is the first level that could affect the availability of data because it is an outage that causes the connection between the storage server and the systems being used to access the data. This could occur because of server malfunction that shuts down the server. This could occur on wired computers if the connection cable between the computer and the switch gets disconnected. This could occur on wireless systems if the server WIFI connector malfunctions.

An additional hazardous event that could occur that could affect the accessibility of available patient data is internet loss. This could result from a simple problem such as being in an area of the institution that has bad signa, to the modem and routers being out of service or a damaged internet line underground. Typically, desktops are hardwired into the internet connection but may facilities use iPads, tablets, and laptops to complete their work. If the internet is not accessible, a caretaker cannot pull information from the servers where patient data is stored. Without this information, caretakers cannot properly manage patient care.

Finally, a full-blown power outage across a hospital can shut down multiple functions within the hospital including access to patient data. If the generators fail, there will be no way to access the data from the server whether directly or indirectly. Healthcare professionals can still perform basic care on a patient but can't access any background information or administer any medications. A blackout will also result in full shut down of accessibility to patient information. Finally, if the hospital has an uninterrupted power supply (UPS) set up and that fails, there will be no backup power and all access to patient information will be shut down.

6.1.2 Data Integrity & Protection from Theft

Our first hazardous event that can occur is if information is stolen by an internal employee. An agitated employee may want to get back at any employers for wrongful termination or if they were acted upon negatively. Employees with access to information may steal the information stored. Additionally, if an employee who doesn't have access to a family member/friend may choose to take information.

Another hazardous event that can threaten the integrity or safety of patient data is a hacking situation from an external source. Ransomware, viruses, and worms could possible enter the system and attack it. Even if the hacker doesn't have access to files, they may send in phishing emails to gain access to an employee's computer. If a hacker gains access to the system data may be stolen, systems may be shut down, etc.

Finally, dual-company ownership can make a healthcare institution at risk for data being compromised. Dual-ownership can result in more individuals than necessary having access to patient data and other data within the institution. If privileges aren't assigned correctly, then the possibility of having an individual who doesn't need the data being given access increases. The individuals with access needs to be strictly set to only necessary personnel to reduce the risk of data being compromised or stolen.

6.1.3 Physical System Protection

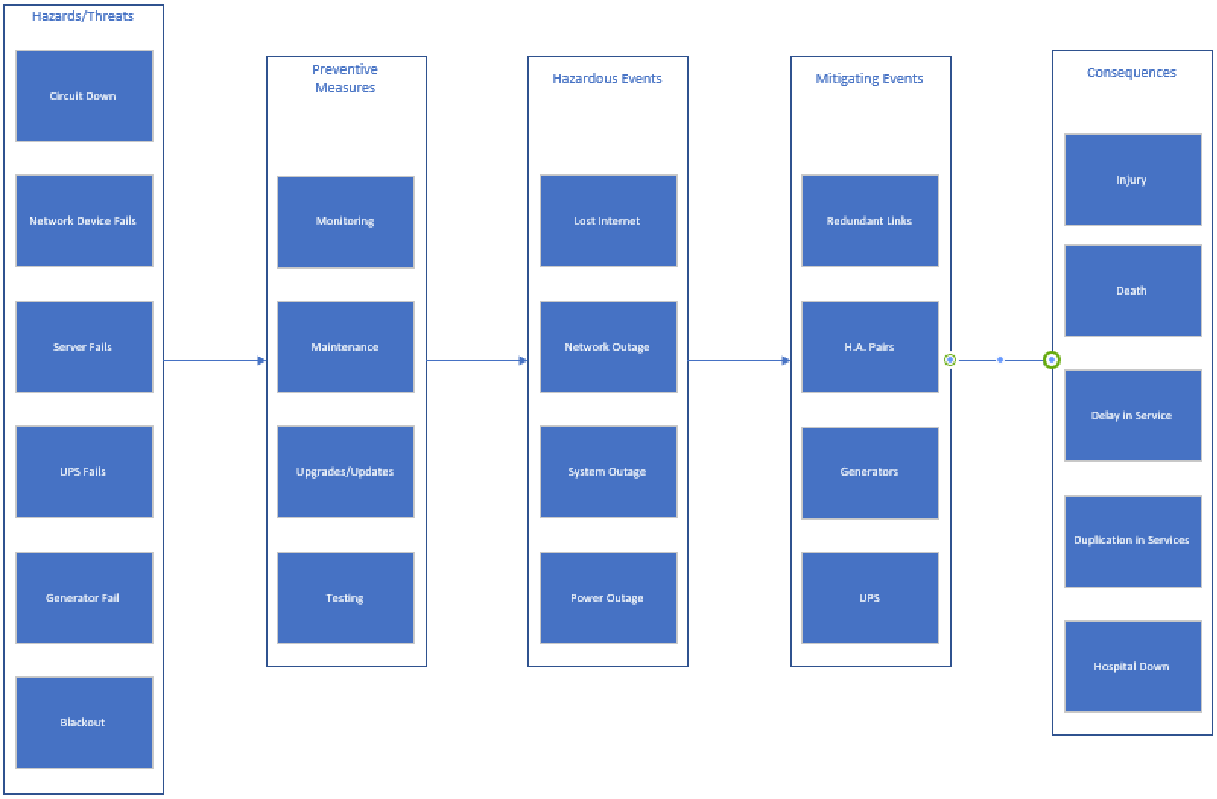
Our first hazardous event that can affect the physical system housing patient data is a data center power failure. This could result if not enough power is going to the server room causing a breakdown of the cooling system and eventually the hardware. Another way this could occur is if there is too much power going through the systems, overloading the generator and then eventually breaking which causes the breakdown of hardware. Natural disasters, e.g. thunderstorms, hurricanes, can cause power outage where it strikes the building and overloads the generator which causes the power to shut down.

An additional hazardous event that can affect the physical system housing patient data is a fire in the server room. Build-up of heat in the server room can cause an explosion. Cables not correctly organized and placed away can block the main ventilator of the server motherboard that can cause the motherboard to melt and break. Additionally, cooling system failure can cause the room to heat up to the point of meltdown/explosion. Faulty battery in the main generator can also cause an explosion. A massive power surge can also occur and can go straight to the server room causing everything to overheat.

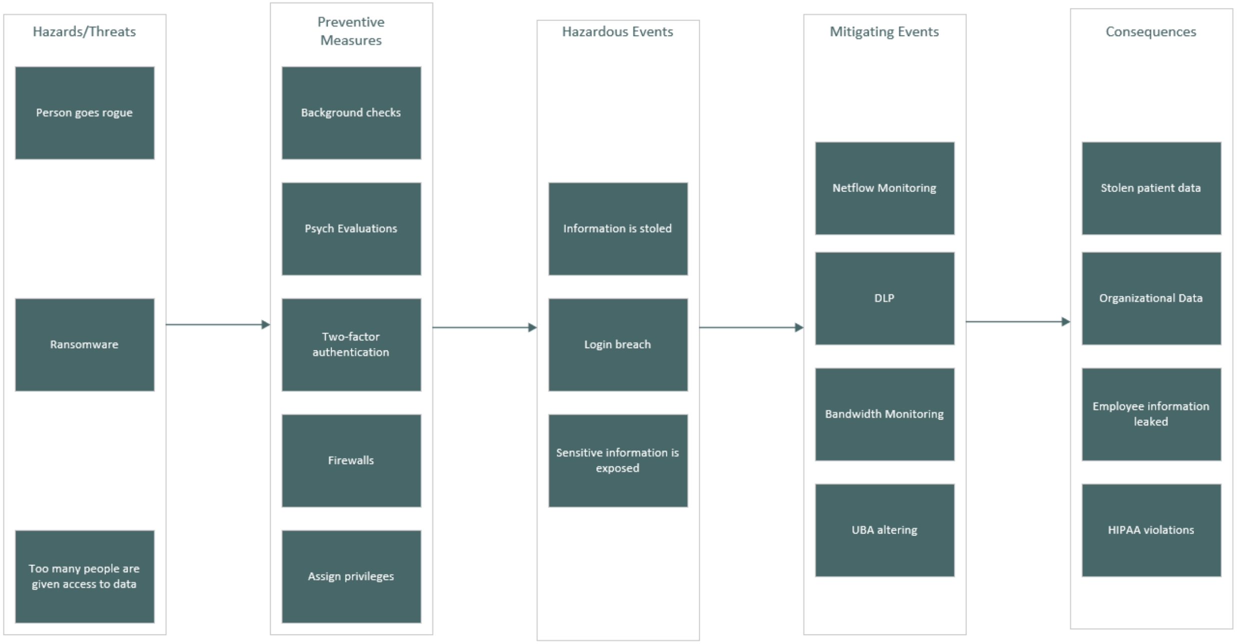
IT human errors can result in damage to the physical systems housing patient data. If IT personnel do not upkeep systems, the systems can fail. Not replacing old cooling systems can result in their failure which could then result in damage to the system. If the server rooms are kept clean from dust, that can increase the risk of fire. IT workers not being careful while in the server room can result in them tripping and shutting down an entire server by shutting off the power to the system. Mismanagement of cables and incorrect labeling can result in an IT worker moving or disconnecting the incorrect cables causing system shutdown.

6.2 Bow-Tie Diagrams

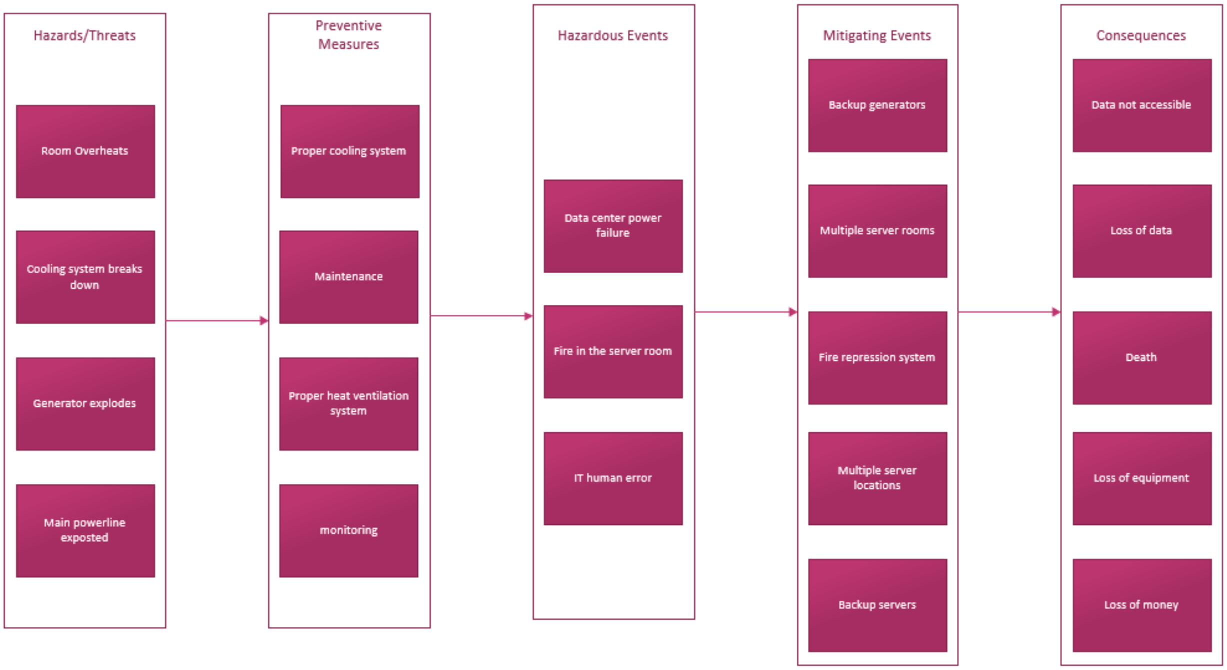
6.2.1 Data Accessibility/Availability



6.2.2 Data Integrity & Protection from Theft



6.2.3 Physical System Protection



6.3 Risk Influencing Factors

6.3.1 Data Accessible/Available

Many factors affect the likelihood of hazardous events occurring including operation, organizational and regulatory. The following are the RIFs for Data Accessibility/Availability:

- Operational
  - Monitoring
  - Maintenance
  - Disaster recovery test
  - Business continuity plan
- Organizational
  - Architecture
    - Resiliency
    - DR Plans
    - Redundancy
  - Disaster recovery test requirements
- Regulatory
  - MACRA
  - HITECH Act
  - HIPAA

6.3.2 Data Integrity & Protection from Theft

There are multiple risk influencing factors that could increase the risk of patient data being compromised or stolen. The following are the RIFs for Data integrity & protection from theft:

- Operational
    - System checks
    - Set-up standards and procedures for data breaches
    - Having authentication methods for users
    - Back-up servers
- Organization
    - Server maintenance
    - Update devices and machines
    - Business continuity plans
- Regulatory
    - HITECH act
    - HIPAA

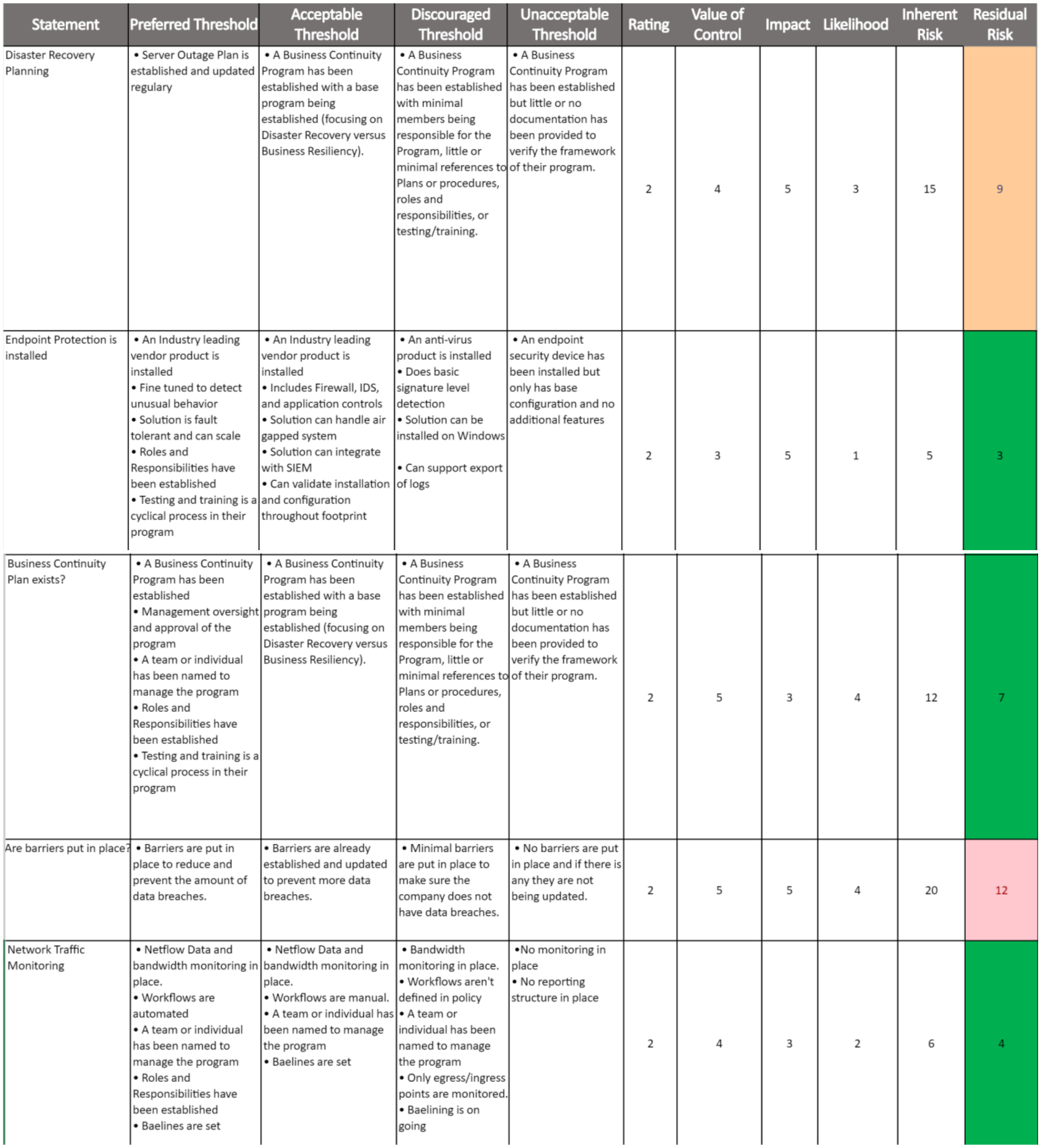
6.3.3 Physical System Protection

Many operational, organizational, and regulatory factors can affect the likelihood of a hazardous event occurring. The following are the RIFs for Physical System Protection:

- Operational
    - Constant checks on server systems
    - Proper care of the server room
    - Proper maintenance of the cooling system
    - Proper maintenance of the ventilation system
    - Mandatory updates on equipment's
    - Proper care of generator
- Organizational
    - Routinely checks on server maintenance
    - Proper cable and airflow management in the server room
    - Routinely check on generators
- Regulatory
    - HITECH Act
    - HIPAA

6.4 Qualitative/Semi-Quantitative Analysis

The following chart contains the qualitative/semi-quantitative analysis. The actual excel document can be found in the document repository.



Statement	Preferred Threshold	Acceptable Threshold	Discouraged Threshold	Unacceptable Threshold	Rating	Value of Control	Impact	Likelihood	Inherent Risk	Residual Risk
Disaster Recovery Planning	• Server Outage Plan is established and updated regulary	• A Business Continuity Program has been established with a base program being established (focusing on Disaster Recovery versus Business Resiliency).	• A Business Continuity Program has been established with minimal members being responsible for the Program, little or minimal references to Plans or procedures, roles and responsibilities, or testing/training.	• A Business Continuity Program has been established but little or no documentation has been provided to verify the framework of their program.	2	4	5	3	15	9
Endpoint Protection is installed	• An Industry leading vendor product is installed • Fine tuned to detect unusual behavior • Solution is fault tolerant and can scale • Roles and Responsibilities have been established • Testing and training is a cyclical process in their program	• An Industry leading vendor product is installed • Includes Firewall, IDS, and application controls • Solution can handle air gapped system • Solution can integrate with SIEM • Can validate installation and configuration throughout footprint	• An anti-virus product is installed • Does basic signature level detection • Solution can be installed on Windows • Can support export of logs	• An endpoint security device has been installed but only has base configuration and no additional features	2	3	5	1	5	3
Business Continuity Plan exists?	• A Business Continuity Program has been established • Management oversight and approval of the program • A team or individual has been named to manage the program • Roles and Responsibilities have been established • Testing and training is a cyclical process in their program	• A Business Continuity Program has been established with a base program being established (focusing on Disaster Recovery versus Business Resiliency).	• A Business Continuity Program has been established with minimal members being responsible for the Program, little or minimal references to Plans or procedures, roles and responsibilities, or testing/training.	• A Business Continuity Program has been established but little or no documentation has been provided to verify the framework of their program.	2	5	3	4	12	7
Are barriers put in place?	• Barriers are put in place to reduce and prevent the amount of data breaches.	• Barriers are already established and updated to prevent more data breaches.	• Minimal barriers are put in place to make sure the company does not have data breaches.	• No barriers are put in place and if there is any they are not being updated.	2	5	5	4	20	12
Network Traffic Monitoring	• Netflow Data and bandwidth monitoring in place. • Workflows are automated • A team or individual has been named to manage the program • Roles and Responsibilities have been established • Baelines are set	• Netflow Data and bandwidth monitoring in place. • Workflows are manual. • A team or individual has been named to manage the program • Baelines are set	• Bandwidth monitoring in place. • Workflows aren't defined in policy • A team or individual has been named to manage the program • Only egress/ingress points are monitored. • Baelining is on going	•No monitoring in place • No reporting structure in place	2	4	3	2	6	4

6.5 Data Dossier

Data Dossier	
Component: Generator shuts down	**System:** Server outage
Description: The server that provides connections to all computers in the network is used every day in order for proper business to run. The generator is used to keep all power online within the hospital and make sure the business is running as usual. Both are stored in a secure location where only certain individuals are allowed entry. It is also sheltered away from any environmental damage.	

Failure Mode: ∉ Human Error with dealing with generator ∉ Generator has a fire ∉ Generator has hardware failure **Failure Rate (per hour):** ∉ 1.7 x 10^{-5} ∉ 1.0 x 10^{-5} ∉ 2.8 x 10^{-5} **Source:** https://venturebeat.com/2012/11/14/the-high-cost-of-server-downtime-infographic/
Assessment: The failure rates are based upon the sources. Taking the percentage per year, dividing the percentage by 365, and then dividing by 24 to get the failure rate per hour. The findings show that there is a higher chance of a hardware failure happening compared to any other incidents per year. The source also goes into details about the losses that happen when an incident occurs and the money lost.
Testing and Maintenance: The generator should be tested, monitored, and maintained at least once every year. The test should cover what happens to the server and if a backup generator will immediately turn on or not. Any possible failures that happen during testing should be fixed immediately and maintained so that it is back in "brand new" condition.
Comments:

6.6 Accident Scenarios & Causal/Frequency Analysis

6.6.1 Data Accessibility/Availability

The following is an accident scenario including the cause and effects that would affect the availability of accessible data.

1. Car hits electric pole outside of hospital
2. Primary circuit goes down
3. Monitoring detects outage
4. Automatic failover fails
5. Systems become unavailable
6. EMS cannot communicate with hospital
7. Ambulances rerouted – possible death/injury
8. Teams engaged fail over manually

6.6.2 Data Integrity & Protection from Theft

The following is an accident scenario including the cause and effects that would affect the integrity or protection of electronic patient data.

1. Employee opens phishing email
2. Malware downloaded to machine
3. Malware is executed
4. Malware propagates unsecured endpoints

5. Malware encrypts unstructured data

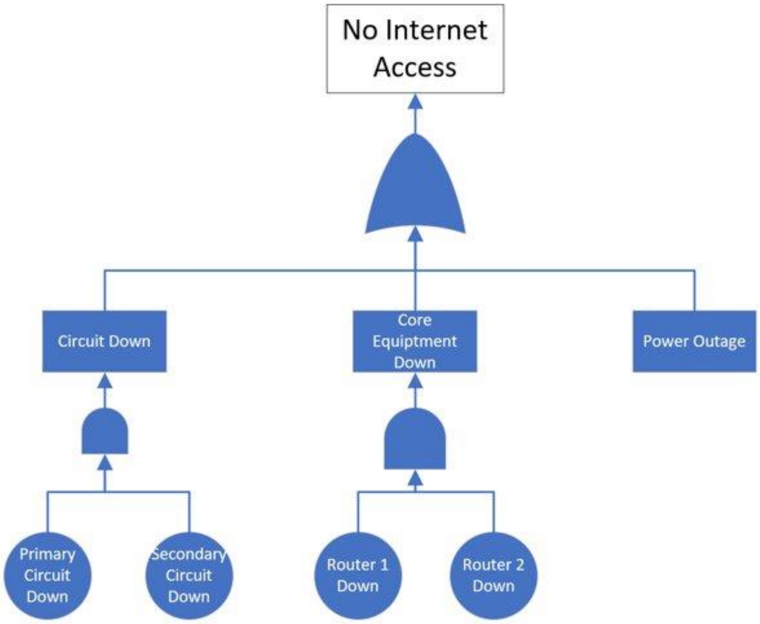
6.6.3 Physical System Protection

The following is an accident scenario including the cause and effects that would affect the integrity or protection of electronic patient data.

1. Maintenance on cooling systems was not complete
2. Cords bunched up near ventilation areas
3. Dust accumulates in server room
4. Server overheats
5. Fire starts
6. Hardware breaks down
7. Fire spreads to the rest of the building
8. Server outages
9. Massive loss of data
10. Loss of income
11. Potential loss of life

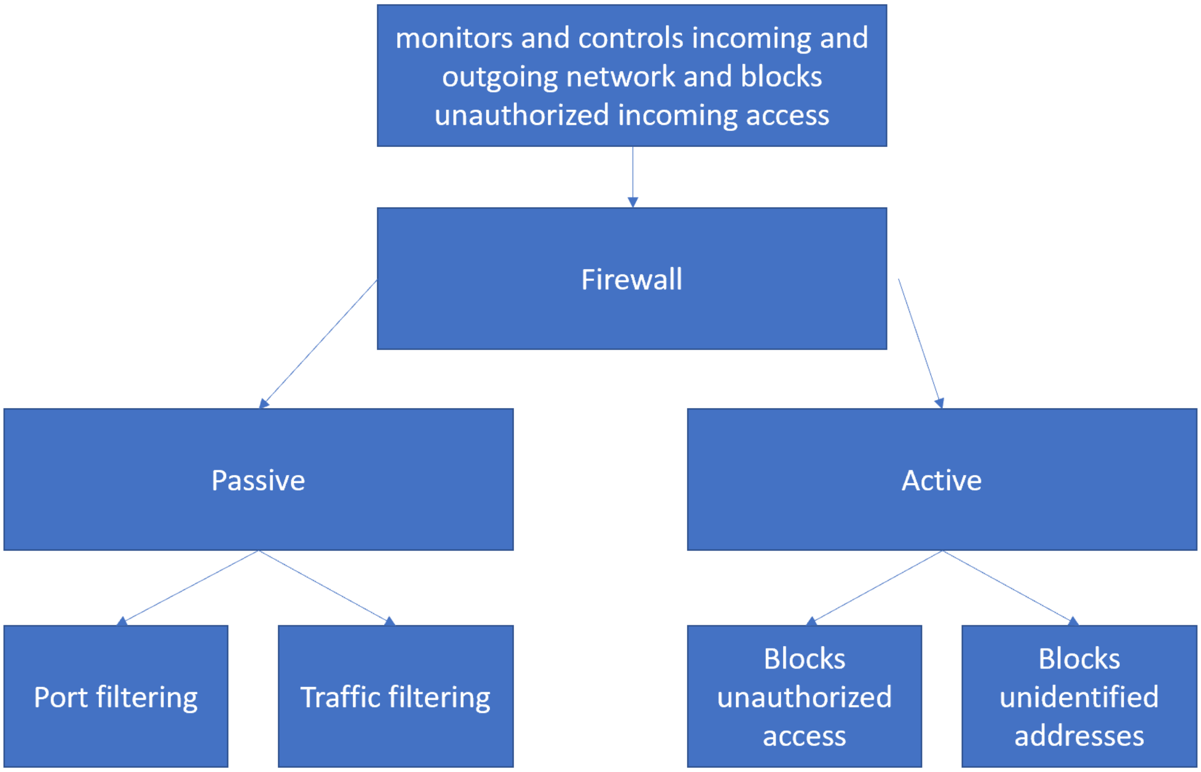
6.7 Fault Tree Analysis

Fault Tree analysis is used to determine the root cause of a hazardous event. This is a root cause analysis for there being no internet access in the hospital. See the fault tree diagram below.



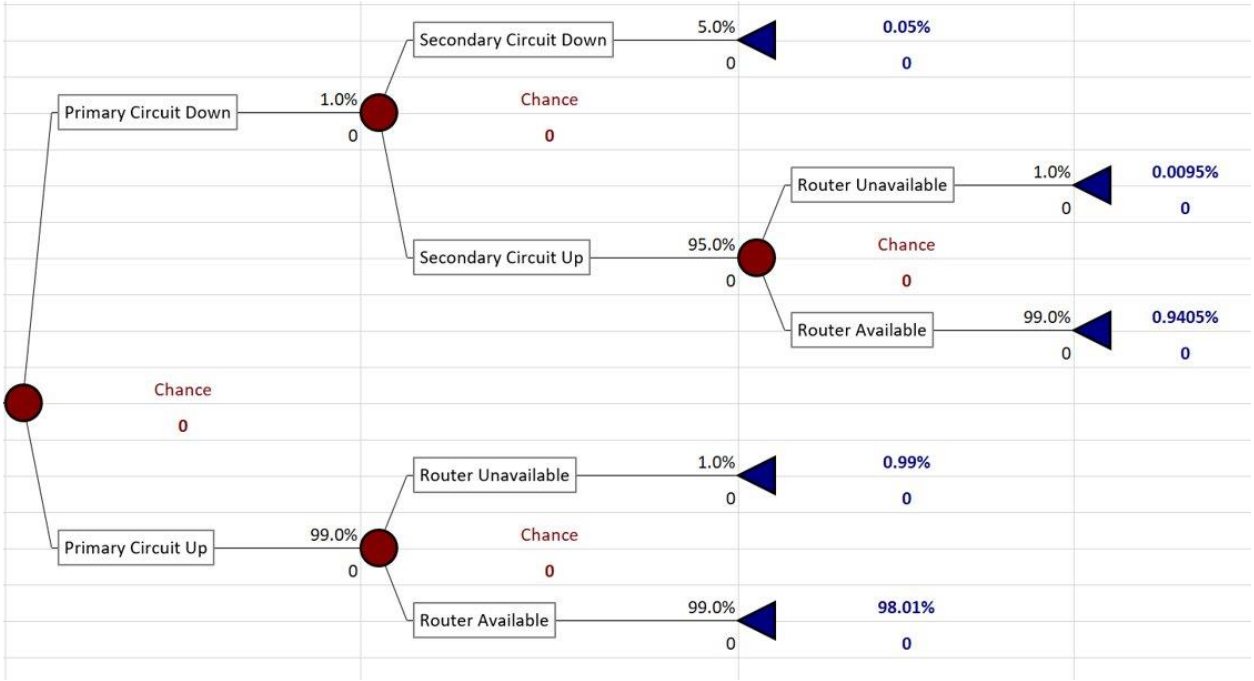
6.8 Hazard/Barrier Matrices

Here is a hazard/barrier diagram/matrix for a firewall. Firewalls monitor and control incoming and outgoing network and blocks unauthorized incoming access. Passive functions are port filtering and traffic filtering. Active functions include blocking unauthorized access and blocking unidentified addresses.


monitors and controls incoming and outgoing network and blocks unauthorized incoming access
Firewall
Passive
Active
Port filtering
Traffic filtering
Blocks unauthorized access
Blocks unidentified addresses

6.9 Event Tree Analysis

Below is the event tree analysis for effects of a power outage on availability of patient data. Specifically, the likelihood of the circuit and router being down. There is less than a 2% chance that something goes wrong.

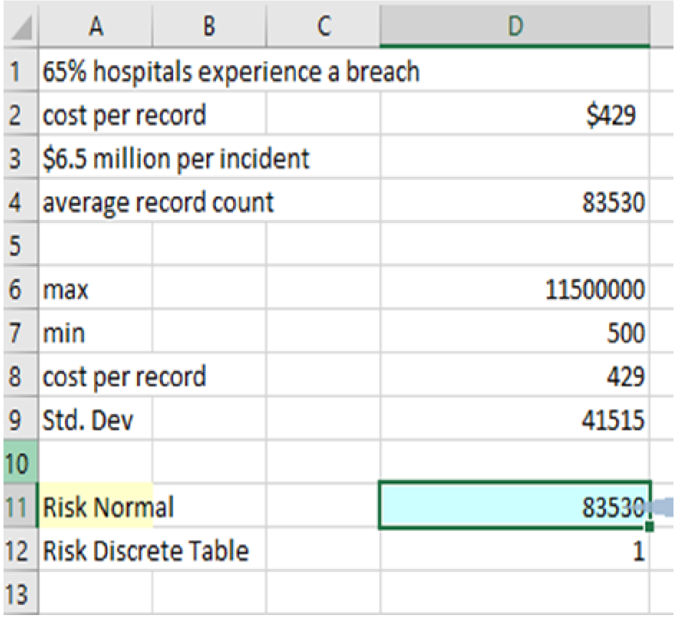


6.10 Quantitative Risk Analysis

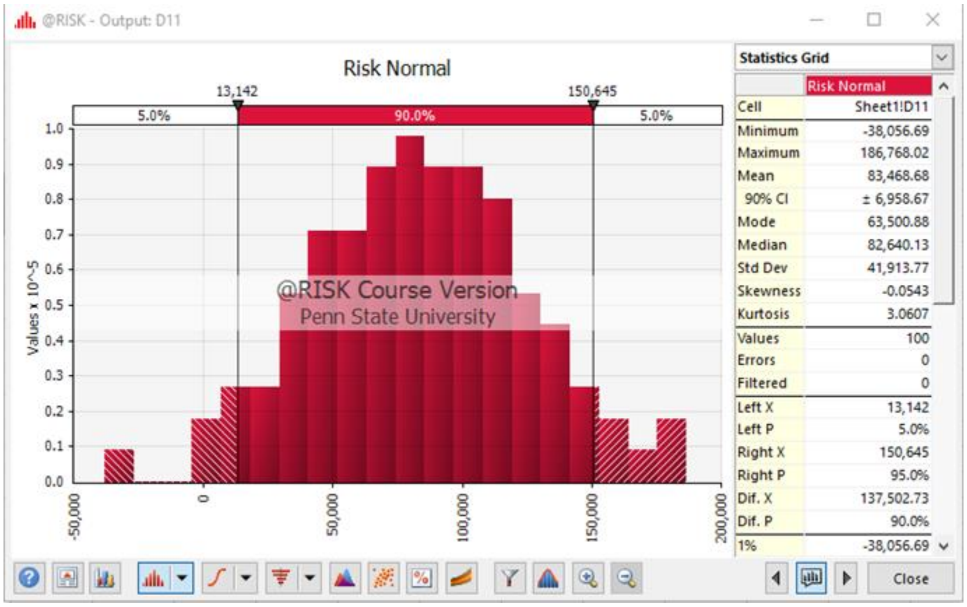
Our quantitative risk analysis was based on data collected regarding hospital breaches and the cost of those breaches. On average, the cost per record breaches is $429 dollars. The average amount of record impacted during a breach is 83,530. The max amount of records breached is 1,150,000 and the minimum amount is 500 and a standard deviation of 41,515.

Our formula for row 11 is =@RiskOutput()+((@RiskNormal(90,45))/180)*2500000*429

Our formula for row 12 is =@RiskOutput()+@RiskDiscrete({1,0},{0.65,0.35})



	A	B	C	D
1	65% hospitals experience a breach			
2	cost per record			$429
3	$6.5 million per incident			
4	average record count			83530
5				
6	max			11500000
7	min			500
8	cost per record			429
9	Std. Dev			41515
10				
11	Risk Normal			83530
12	Risk Discrete Table			1
13				



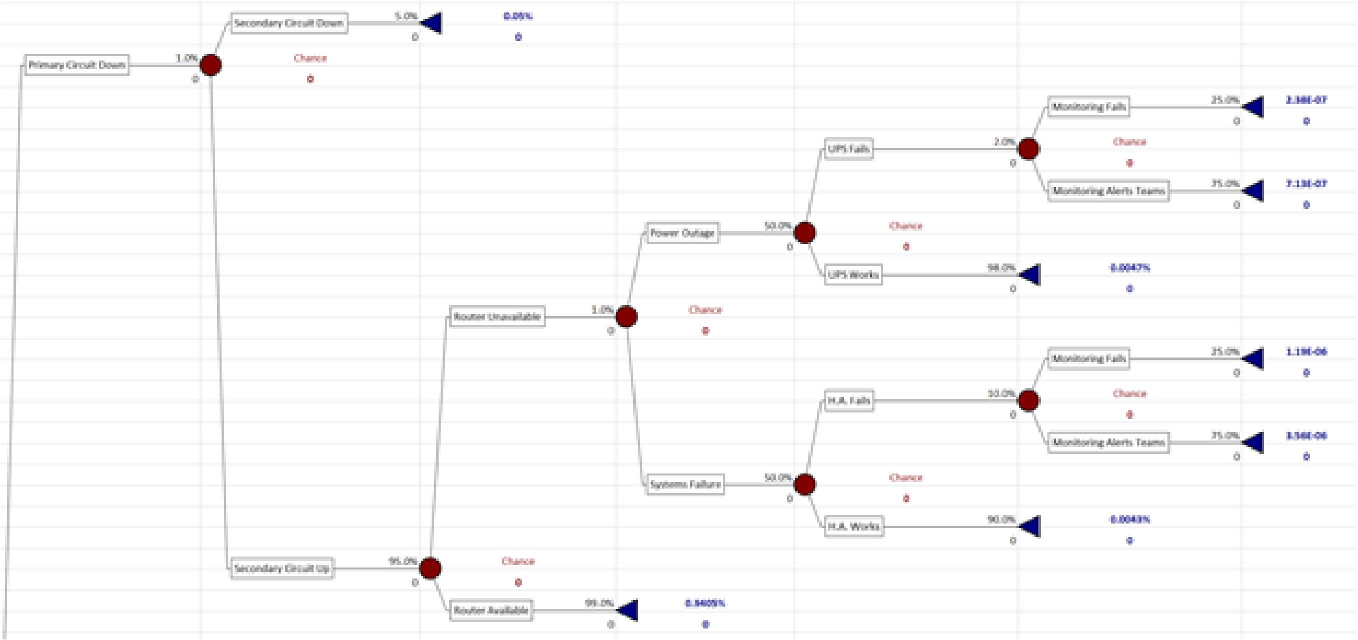
Statistics Grid

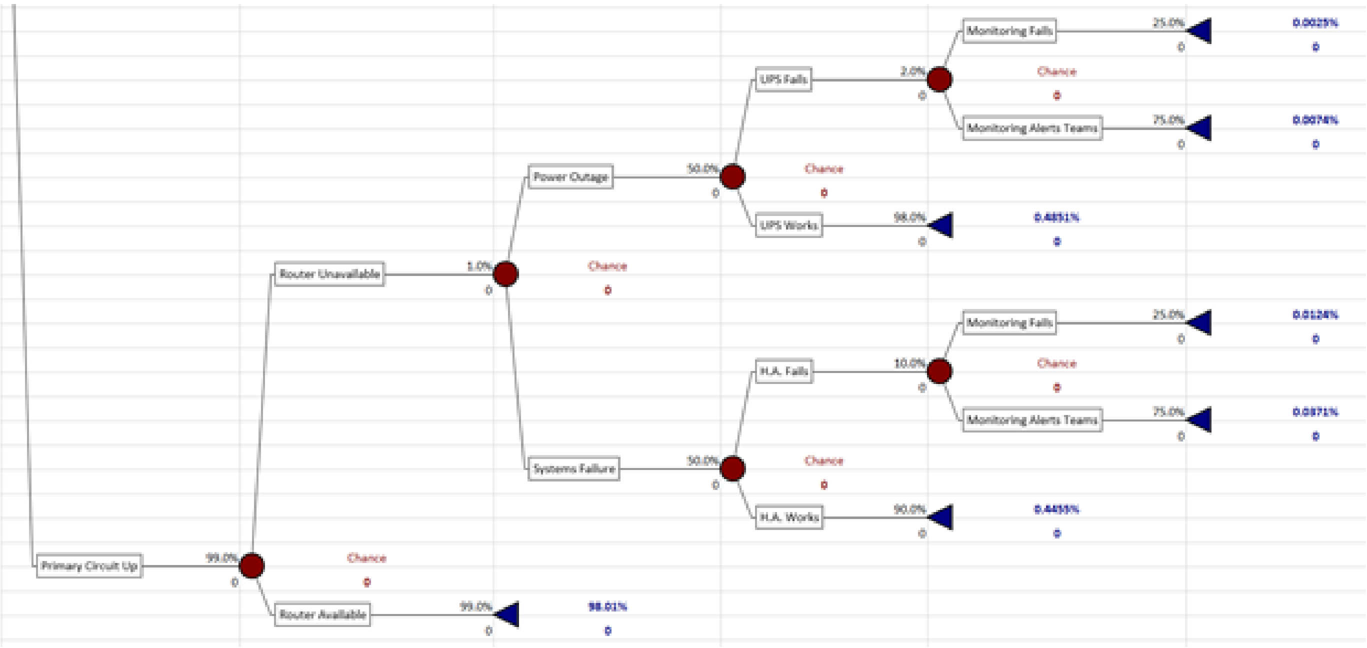
	Risk Normal
Cell	Sheet1!D11
Minimum	-38,056.69
Maximum	186,768.02
Mean	83,468.68
90% CI	± 6,958.67
Mode	63,500.88
Median	82,640.13
Std Dev	41,913.77
Skewness	-0.0543
Kurtosis	3.0607
Values	100
Errors	0
Filtered	0
Left X	13,142
Left P	5.0%
Right X	150,645
Right P	95.0%
Dif. X	137,502.73
Dif. P	90.0%
1%	-38,056.69

6.11 Event Tree Rerun

Following the implementation of mitigation measures/controls, we reran the event tree to determine the probability of hazardous event in regards to availability of patient data.

Note: This is split into two images.





References

(1) https://www.hipaajournal.com/2019-cost-of-a-data-breach-study-healthcare-data-breach-costs/

(2) https://www.hcinnovationgroup.com/clinical-it/news/13029134/survey-nearly-all-us-hospitals-use-ehrs-cpoe-systems