UrRISK04

SRA 311.001

Fall 2014

Table/Row # 3

Dennis Czaplicki [dmc5645]

Lindsay Henzes [lvh5197]

Table of Contents

TIP

To update the above “table of contents” (TOC), simply 1) Right-click the TOC, 2) Select “Update Field,” and 3) “Update Entire Table.” Note that typing on this TOC will not work!

This TOC is linked to Word Styles **Heading1** and **Heading2** that appear in the paper

I. Introduction

Analyzing risk remains a cornerstone in the running of any business or infrastructure in today's world. Hazards exist all around us, but only the most trained analytical minds will be able to identify them and thus be able to plan ahead for them. Today's health care systems are a critical part of our society, so it is important that they stay up and running all the time with minimal problems. In order to ensure this happens, the risks of running a health care system such as a medical center or hospital need to be accounted for to prevent disasters from happening. This is vital to take preventative steps towards these risks because once it has happened, it is far too late. MUST FIX THISSSSS

A) Purpose

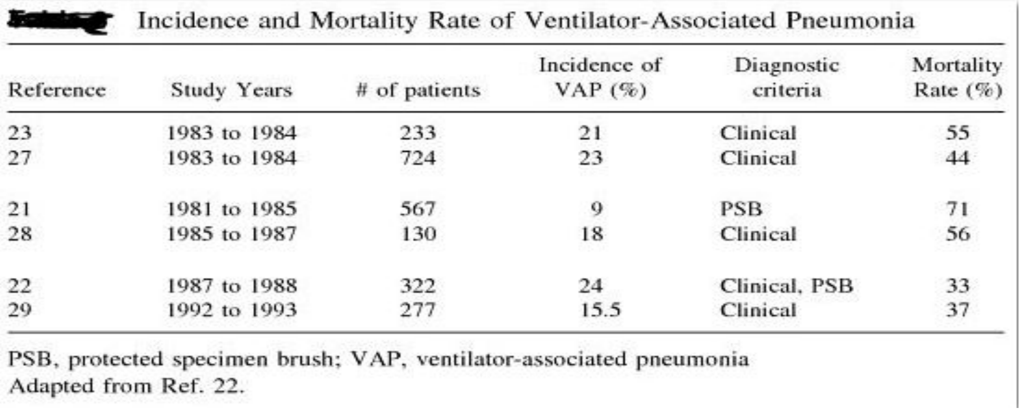
This risk assessment will focus on Mount Nittany Medical Center, a 260 bed facility that serves the medical needs of both State College and its surrounding areas from the point of view as an admitted hospital patient. This report will spotlight the different potential risks an admitted patient at Mount Nittany could face and identify steps in preventing them. By managing the different potential risks, we can prevent Mount Nittany from contributing to the 55.6 billion dollar medical liability bill that hospitals face annually (Mello, Chandra, Gawande, Studdert 2011).

B) Scope of the Risk Assessment

There are many different types of risks that a hospital can face and they are often grouped into different categories. According to Doctors Bonnie Henry and Brian Schwartz in a presentation for the Disaster Preparedness Conference in 2006, the types of risks for a hospital and a patient include: Naturally occurring events, technological events, human related events, and events involving hazardous materials (Henry, Schwartz 2006).

Using the 4-Step Risk Assessment Process, as shown in Figure 1**,** a few key risks have been identified and observations will be based off of the identified risks. These include:

Contracting Pneumonia: When a patient checks into a hospital, they are focused on curing or fixing the problem they came to the hospital to address. Patients will often contract an infection of some sort during their hospital stay. A common infection that can affect patients at Mount Nittany Medical Center is pneumonia because they have ventilators there. According to an article in Forbes, ventilators are breeding grounds for germs that will eventually find their way into a patient's lungs (Herper 2007). The National Library of Medicine also states that hospital-acquired pneumonia (HAP) can be passed through the health care workers themselves or from patient to patient. When an infection like this spreads to patients whom are already weakened, the results can be fatal in anywhere from 33%-71% of cases meaning it is extremely dangerous and should be planned for as much as possible (Keita-Perse, Gaynes 1996). Error! Reference source not found. Table 1 presents more statistics on the fatality of Ventilator-Associated Pneumonia.



[redacted] Incidence and Mortality Rate of Ventilator-Associated Pneumonia

Reference	Study Years	# of patients	Incidence of VAP (%)	Diagnostic criteria	Mortality Rate (%)
23	1983 to 1984	233	21	Clinical	55
27	1983 to 1984	724	23	Clinical	44
21	1981 to 1985	567	9	PSB	71
28	1985 to 1987	130	18	Clinical	56
22	1987 to 1988	322	24	Clinical, PSB	33
29	1992 to 1993	277	15.5	Clinical	37

PSB, protected specimen brush; VAP, ventilator-associated pneumonia
Adapted from Ref. 22.

Table 1: Incidence and Mortality Rate of Ventilator-Associated Pneumonia

Cyber Attack: Admission into a hospital as a patient requires giving personal information including first and last name, phone number, email, and insurance (if the patient has insurance). All of this information is stored in a record on the hospital's database. The patient's health record is always at risk of being exposed by a cyber-attack. According to the Canadian Medical Association Journal more than 7 million health records in the United States alone were compromised by data breaches in 2013. According to a report by Redspin, an information security company, this number increased by 137% from the previous year. This increase in affected health records is predicted to continue to rise as hospitals move towards more online collections of health records (Collier 2014).

Incorrect Diagnosis: Going into a hospital involves requires that the patient trust the doctor's ability to correctly diagnose them. On occasion the doctor misdiagnoses the patient and the results are deadly. According to a study from the Journal BMJ Quality and Safety each year an estimated 5% of adults are misdiagnosed based on currently available evidence. This rate, although seemingly low, actually calculates to about 12 million misdiagnosed adults per year (Singh 2014). A misdiagnosed patient could lead to being given the wrong medication, which could potentially prolong the original problem for the patient. The patient takes a serious risk going to the hospital and putting their trust in the Doctor's judgment of their diagnosis.

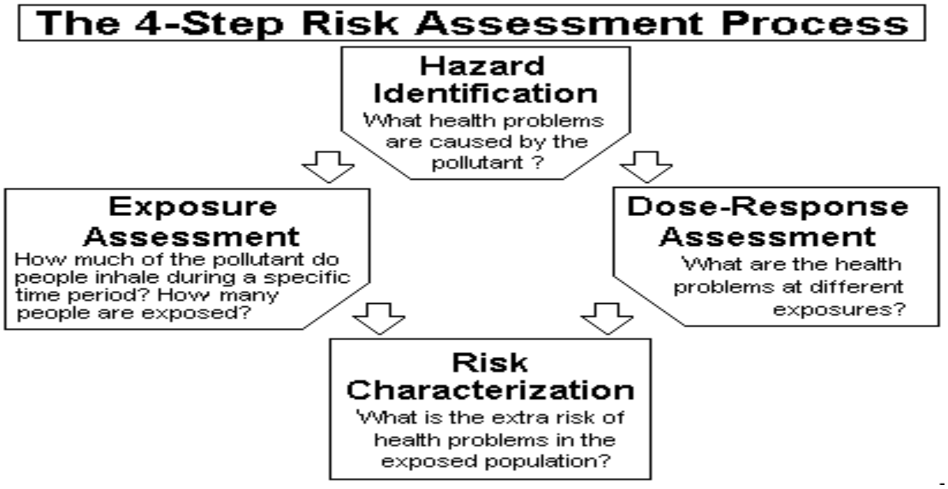

The 4-Step Risk Assessment Process
Hazard Identification
What health problems are caused by the pollutant ?
Exposure Assessment
How much of the pollutant do people inhale during a specific time period? How many people are exposed?
Dose-Response Assessment
What are the health problems at different exposures?
Risk Characterization
What is the extra risk of health problems in the exposed population?

Figure 1: The Four-Step Risk Assessment Process (McGill, 2010, p. 1)

II. Risk Assessment Approach

Bringing in a qualified team is an important step in a risk assessment process. By bringing in the best risk consultants available, you are able to get the best and most accurate assessment possible. Our consulting team consists of two students: Dennis Czaplicki and Lindsay Henzes, two very sought after SRA students.

Dennis is a junior at Penn State University in which he is studying Security and Risk Analysis. He has taken a variety of courses offered at Penn State that are going to be applied throughout the risk assessment. Classes like Statistics 200 and SRA 497A are two intermediate level statistics courses that will allow him to perform statistical analysis on data found in order to get a quantitative measure of certain risks and their prevalence. Dennis is also currently enrolled in SRA 311 which is a Risk Management course. This will be of much help and importance to the risk assessment because it will allow for the best methods of identifying and assessing risks to take place. Finally, Dennis has also been selected to do more consulting work for PricewaterhouseCoopers in the upcoming summer thus proving his competency to compile both a thorough and analytical risk assessment.

Lindsay is a junior at Penn State University majoring in Security and Risk Analysis. As the major title indicates, Lindsay has taken many courses which have focused on methods of risk assessment. Past classes which have been of much help to Lindsay’s risk assessment abilities include SRA 231 and Statistics 200. SRA 231 provided and overview and tutorials on the importance of using risk matrices to calculate the probability and impact of risks. Statistics 200 along with SRA 497A, a statistics class with a focus in information sciences that she is currently enrolled in, have taught Lindsay the importance of qualitative and quantitative data analysis and using these analyses for real life situations, including risk assessment. Lindsay is also enrolled in SRA 311 which is a Risk Management course with an emphasis on mitigation and assessment. SRA 311, so far, has taught Lindsay necessary steps and methods for risk identification and assessment.

For this risk assessment, it was that essential to identify some of the main hazards that a patient from Mount Nittany Medical Center could potentially face. In order to make sure this is done correctly, the hazard identification process was broken down into three subparts: literature review, structured analytics, and a virtual site visit.

Literature Review

One of the best ways to identify hazards is to look at previous incident logs or in our case, past events of scenarios similar to the ones being focused on. By doing this, you are allowing yourself to look at either successes or failures from the past, and seeing what they did right or wrong so you can thus build off of that. Numerous sources of literature were examined that have looked into the three different risks that have been identified that a patient at Mount Nittany could which include: contracting pneumonia, a cyber-attack on patient health records, and an incorrect diagnosis. Some of these sources include an article from the Canadian Medical Association about the increase in cyber breaches (Collier 2014) and even a Wall Street Journal article about the battle against doctors misdiagnosing patients (Singh 2014). By reviewing this literature, the team was able to gain as much knowledge on the issues at hand and look at past cases of the incidents. Upon doing this, better solutions were generated regarding how to prevent or manage these risks.

Structured Analytics

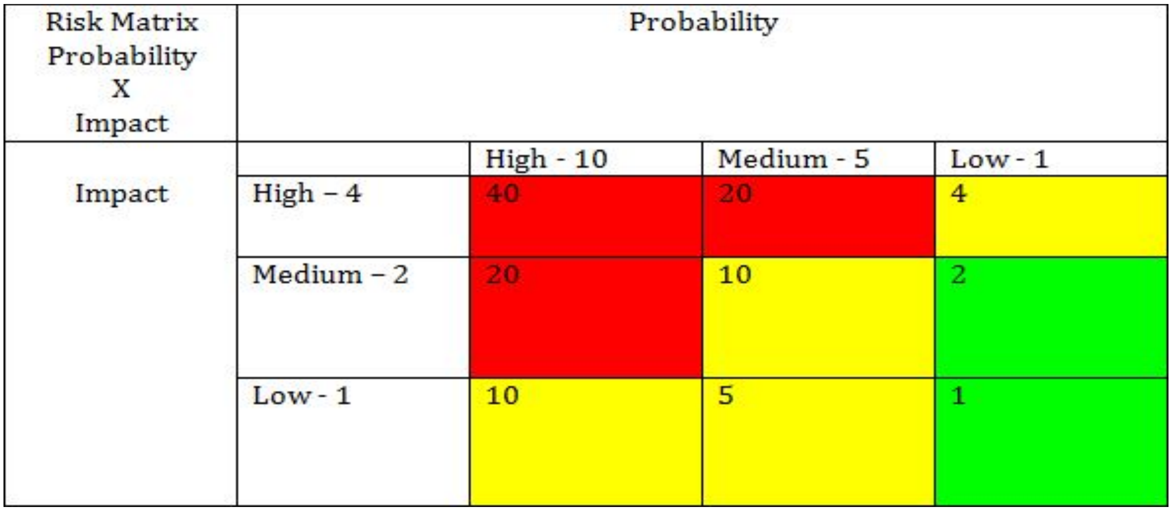
With structured analytics, the team began to brainstorm the different risks that a patient could potentially face. A key way to brainstorm as many risks as possible is to use a divergent form of thinking. Using this form of thinking, team members basically spoke freely and wrote down any idea that came to mind without thinking too much into it. You can refer to **Attachment 2** to see the full list of risks generated via divergent thinking. Once a big list of ideas was generated, the list needed to be narrowed down and to decide which risks most applied to a patient of Mount Nittany. Risks were then examined more critically and assessed to see which risks would fall into the scope being examined. Looking back at **Attachment 2**, you can then see the convergent thinking results that were generated. These ideas are much more oriented with what the team was thinking.

Virtual Site Visit

Lastly, there was an important site visit. Doing site visits are very important because they allow the assessor to get a first-hand look at the facility they are performing the risk assessment for. In this case, the team has been to Mount Nittany Medical Center so they are quite familiar with the facility itself. This is important in the sense that they can visualize the risks being examined, in person. For example, one of the risks being assessed is a patient contracting pneumonia during their stay mostly through a ventilator. By walking around Mount Nittany, the assessor can see firsthand how the ventilators are both sanitized and how often different patients use the same ventilator in a certain amount of time. Looking at pictures online can also sufficiently suffice when doing a site visit in person is not feasible for some reason or another. Doing this virtual site visit helped the team to remember certain details about the facility that are included in the assessment.

Figure 2 - Risk Matrix to evaluate potential risks identified below portrays the risk matrix that will be using to determine the likelihood and impacts of the risks for this report. The regions of the matrix shaded in **red** are higher probability and higher impact. For these risks, it is recommended to transfer

these risks by contracting them out to a third party who will take care of them. The regions of the matrix shaded in **yellow** are moderate probability and moderate impact. It is recommended to mitigate these risks, for example having a plan in set for immediate recovery of exploited hospital records by a cyber-security threat. The regions of the matrix shaded in **green** are low probability and low impact risks. The best way to respond to these risks is to accept them for they are not likely to happen and if/when they do occur the impact is not extremely significant.



Risk Matrix Probability X Impact	Probability			
		High - 10	Medium - 5	Low - 1
Impact	High – 4	40	20	4
	Medium – 2	20	10	2
	Low - 1	10	5	1

Figure 2 - Risk Matrix to evaluate potential risks identified

III. System Characterization

The system that will be evaluated using the input-process-out IPO model is composed of the cyber security risks the patients are exposed to upon sharing personal information with Nittany Medical Hospital. The cyber security risks the patients face include the possibility of the exploitation of personal information and past hospital records.

In this case, as shown in Figure 3 below, the input is the information supplied by the patient; include first and last name, phone number, email, insurance, and various other forms of personal identification. The process is done when the information is entered into Mount Nittany's Medical System and successfully entered into the online database. The output of this situation is the retrieval of the personal information and hospital records at a later date.

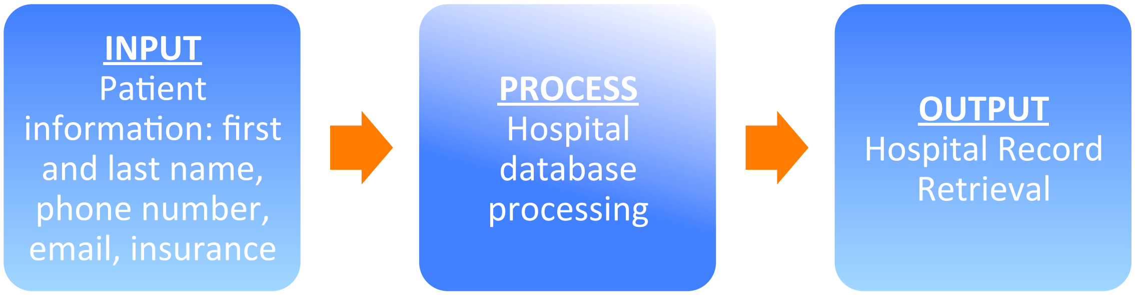

INPUT
Patient information: first and last name, phone number, email, insurance
PROCESS
Hospital database processing
OUTPUT
Hospital Record Retrieval

Figure 3 - IPO describing a cyber-breach on patient records

IV. Threat Statement

There are three types up threat-sources: natural threats, human threats, and environment threats (NIST 300-30, 2002). In this risk assessment there is a focus on human and environmental threats. **Attachment 3** displays the threats focused on in this risk assessment, the motivation behind the threats, and the actions that would occur if the threat were to occur.

The first threat in this risk assessment is catching pneumonia while admitted in Mount Nittany Medical Center. This threat is considered an environmental threat because the spread of the infection travel from one patient to another through air vents or not properly sanitized parts of the hospital.

The second threat is the risk of a cyber-attack on patient's personal records. The threat of a cyber-attack is considered a human threat due the interaction of humans and computers. A human hack infiltrates Mount Nittany Medical Center's network in order to access and steal the records of the patients' admitted.

The third threat in this risk assessment is an incorrect diagnosis of the patient by the doctor. This threat would also be considered a human threat because it is based off of the doctor's diagnosis of the patient. The incorrect diagnosis could be due to insufficient results of medical tests on the patient, incorrect analysis of the symptoms provided by the patient or lack of knowledge and experience of what the patient describes to the doctor. No matter what the reason behind the misdiagnosis, the patient's life is always put at risk from a common human mistake.

V. Risk Assessment Results

After assessing Mount Nittany Medical Center for a variety of potential risks, the following three risks were the ones deemed most probable to affect an admitted patient. This was determined using a few different factors which included assigning a quantity to each risk in order to determine both its probability and impact. These risks are human and they include:

1. Catching pneumonia while admitted
2. Cyber-attack on patient records
3. A doctor misdiagnosing a patient

A) Threat/Vulnerability Pairs

In order to complete this risk assessment properly it is important to identify the threats posed to Mount Nittany Medical and the corresponding vulnerabilities. A threat is the "potential for a threat-source to successfully exercise a particular vulnerability" and a vulnerability is "flaw or weakness" in the system that "could be exploited by the potential threat-sources" (NIST 800-30, 2002). In this assessment, the main focus will be on the three risks listed in Attachment 3. These three risks will come about via a vulnerability of some sort that is exploited. In the case of catching pneumonia while admitted in the hospital, the vulnerability would be lapses in hospital sanitation and doctor protocols in which the ventilators or rooms were not sanitized nor did the doctor keep the patient moving around to prevent pneumonia. If these manifested itself, that is when the chances of patients getting pneumonia increases significantly. In the next risk, an opening in the hospital's network security would be the vulnerability. These network vulnerabilities are a result of unguarded backdoors in the network security perimeter. These could potentially be exploited by a hacker who wants to acquire patient records. Finally, the last vulnerability of misdiagnosing a patient is a source of Mount Nittany doctors making a mistake in their diagnosis. All of this information can be seen in **Attachment 3** in which it is laid out.

B) Existing Risk Controls

Mount Nittany has some current controls in place regarding their cyber-security. First, authorized users are given a username and password that will allow them to log into the medical center's network, or their intranet. Once inside the intranet, they will need to log in again to another system which will give them access to the patient records. Users must be approved however to gain access to this system which prevents unauthorized users from seeing the sensitive information. There is then a firewall that prevents anyone from attempting to access their internal network via the internet. Finally, any user who attempts to access the Mount Nittany intranet remotely will need to use a small hardware device known as an authentication token that generates a code on it to help gain access to the network (Rouse 2005). This would be an example of two factor authentication.

An attempt to decrease the patients' chances of catching pneumonia during their stay, there are a few controls that have been put in place. The first is to make sure all rooms are sanitized properly and that there is not an excess amount of germs in the rooms or on the ventilators which would increase the chances of catching pneumonia. To keep the rooms clean, a form of Clorox quaternary is most likely used because it has a 99.9% kill rate and kills bacteria in 2 minutes based on research that indicates it is used in over 2500 acute care facilities in the United States (Clorox 2011). For the ventilators, they are sanitized using pressurized heat and disinfectant in order to ensure they are absolutely clean to prevent pneumonia from spreading rapidly through the ventilators.

An existing risk control of incorrect diagnosis of the patient is the doctors, nurses, and all health personnel committed to procedures minimizes any and all medical errors that could lead to misdiagnosis as well as commitment to the procedures of the hospitals, each doctor is hand selected based off of previous education and work experience within the medical field. Past education and work experiences give the doctors, nurses, and other members of the medical staff the credentials to make correct judgments and decisions in regards to the diagnosis of the patients.

C) Likelihood: Discussion and Evaluation

Each vulnerability that is identified in this risk assessment is rated based on the likelihood of the threat exploiting the vulnerability. The ratings of the vulnerabilities were based on a low to medium to high scale. **Attachment 4** rates the vulnerabilities using the likelihood definitions provided in Table 3.4 (2002, 21).

The likelihood of catching pneumonia while admitted into Mount Nittany Medical Center is medium since there is constant sanitization of the hospital. The likelihood of a cyber-attack target the exposure of the patient's is rated as low because there are already sufficient controls in effect, such as the two factor authentication, that have decreased the chance of a successful cyber-attack occurring. Finally, the likelihood for incorrect diagnosis is medium due to the extensive background each doctor has within the medical field and the procedures already set in place.

D) Impact: Discussion and Evaluation

As well as rating the vulnerabilities from a low to medium to high scale, the impact of the vulnerabilities must also be rated to effectively quantify the risk. **Attachment 5** displays the risk scenario and the corresponding vulnerability and impact. The definitions of the levels of impact are based on Table 3-5. The magnitude of impact can be found on page 23 of the NIST 800-30 document.

The definitions of impact provided by NIST helped to classify the impact of catching Pneumonia while admitted in the hospital as medium. Catching Pneumonia while admitted to the hospital is a medium impact because it is not likely to take human life, but rather make the patient's more ill. The impact of a cyber-attack is classified as a medium impact because if the cyber-attack does occur, the patients are not likely to fully trust Mt. Nittany Medical with personal information. In the event of a cyber-attack occurring, it would affect the reputation of Mount Nittany's implemented security procedures and privacy policies. The impact of the incorrect diagnosis of the patient occurring is classified as high impact. This threat is seen as high impact because in the case of misdiagnosis, death is a common outcome due to either inefficient medication causing adverse side effects, or the real diagnosis taking the patient's life (Goldsmith 1997). The deaths of the patients may also lead to different lawsuits from family members of the deceased thus violating Mt. Nittany Medical Center's main interest, which is taking care of the admitted patients.

E) Risk Rating

The Risk matrix in **Attachment 7** was able to yield final results because it allowed for the risks to be quantified. Quantifying the risk involves multiplying the likelihood of threat happening by the impact it would have if it were to occur. This product gives a numerical value for the risk. A range of values was established to determine which values would be considered low, medium, and high. The same was also done for the threat likelihood. In this case for example, a threat likelihood of 1.0 and an impact of 100 would score on the risk matrix while a threat likelihood of 0.25 and an impact of 25 would score low on the risk matrix. Once the product of the likelihood and impact was calculated, it was then placed in a range based on the score. The ranges were: low is 0-24, medium is 25-49, and high is 50-100. The final results of these calculations which are shown in **Attachment 8** are as follows: Cyber-attack on patient records is a low risk at a score of 12.5; catching pneumonia while admitted in the hospital is a medium risk at a score of 25; incorrect diagnosis is a high risk at a score of 50.

F) Recommended Controls

Now that a thorough and proper assessment has been done, three key risks have been identified. With these risks being identified, it is now time to recommend controls to implement for these risks. For the risk of a cyber-attack on a patient's personal records, it is recommended that Mount Nittany accepts this risk. The reason it should be accepted is because it has such a low likelihood since there is very good network security and two factor identifications to ensure only authorized users access the patient records. The impact if it did happen would also only be at a medium impact level because although it could be damaging to a person if their personal information was in the wrong hands, there is still a process for the information to be turned into a monetary gain. For the risk of a patient catching pneumonia during their stay, it would be best if Mount Nittany use the mitigate control because it is a medium level risk. To mitigate the risk, they should develop strict sanitation protocols for the rooms and ventilators that must be followed and continually remind doctors that the patient must be continually moved so fluid does not build up in the lungs. These plans will help lower the risk of a patient catching pneumonia significantly. They can also develop an incident response plan in the event that a patient does catch pneumonia; they will know exactly what to do right away so that they can prevent others from catching it also. Finally, for the misdiagnosing a patient risk, they should avoid this risk all together. This control should be implemented because it is a high level risk ranking medium in likelihood and high in impact. This means that they should restructure their training methods and examinations so that they are much more thorough in how they check a patient. By doing this and taking the extra steps to ensure their diagnosis is correct, they will be able to avoid this high risk.

VI. Summary

Risk assessment is a critical part of today's healthcare system and should be taken very seriously in both how it is conducted and how it is followed up. This risk assessment was done through the point of view of a patient who is admitted into Mount Nittany Medical Center. By setting this scene, it is then possible to narrow down the different risks that could potentially affect the patient. After brainstorming many different risks, the risks that were the focus of the assessment are: catching pneumonia while admitted, cyber-attack on patient records, and a doctor misdiagnosing a patient. Breaking down each of these three risks individually, each risk was given a score based on the product after multiplying the impact score by the likelihood score. The scores were as follows: cyber-attack on patient records with a 12.5, catching pneumonia while admitted with a 25, and being misdiagnosed with a 50. These scores were then put into a category of LOW (0-24), MEDIUM (25-49), or HIGH (50-100). Based off this scale, a cyber-attack was a low risk, catching pneumonia was a medium risk, and being misdiagnosed was a high risk. Now that the three risks were scored and placed into different categories accordingly, it was then time to recommend risks controls based off of the findings. Mount Nittany was recommended to: accept the cyber-attack risk because their current security is sufficient enough and it ranks low in likelihood; mitigate catching pneumonia while admitted by coming up with strict sanitation and doctor protocols and developing an incident response plan if the risk does occur; Avoid doctors misdiagnosing by restructuring training methods and examinations to be more thorough so they can avoid this risk coming up. This information is simplified in a chart in **Attachment 9**.

Reference List

Clorox Professional Products Company Introduces its Newest Non-Bleach Hospital-Use Quaternary Disinfectant Cleaner. (2011, September 26). Retrieved November 17, 2014, from http://investors.thecloroxcompany.com/releasedetail.cfm?ReleaseID=608188

Collier, R. (2014). US health information breaches up 137%. *Canadian Medical Association Journal,* 186(6). Retrieved September 21, 2014, from http://www.cmaj.ca/content/186/6/412.full

Durbin, C. (2003). Hospital breaches of confidentiality. *Chart, 100*(2), 8. Retrieved from http://search.proquest.com/docview/214714018?accountid=13158

Goldsmith, M. F. (1997). National patient safety foundation studies systems. JAMA: The Journal of the American Medical Association, 278(19), 1561-1561. doi:10.1001/jama.278.19.1561

Henry, B & Schwartz, B. (2006). Hospital Risk Assessment [PowerPoint slides]. Retrieved from www.ceep.ca/education/HospitalRiskAssessment.ppt

Herper, M. (2007, June 14). In Pictures: The Seven Scariest Hospital Complications. Retrieved September 21, 2014, from http://www.forbes.com/2007/06/14/hospital-risk-pneumonia-ent-manage-cx_mh_0614riskhospital_slide_6.html

Mello, M., Chandra, A., Gawande, A., & Studdert, D. (2010). National Costs Of The Medical Liability System. Health Affairs, 1569-1577. Retrieved September 21, 2014, from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3048809/

Rouse, M. (2005, September 1). Security token (authentication token). Retrieved October 21, 2014, from http://searchsecurity.techtarget.com/definition/security-token

Singh, H. (2014, Aug 08). The battle against misdiagnosis. *Wall Street Journal* Retrieved from http://search.proquest.com/docview/1551801594?accountid=13158

Stoneburner, G., Goguen, A., & Feringa, A. (2002, July). Risk Management Guide for Information Technology Systems [Electronic version]. National Institute of Standards and Technology, 800(30).

Attachment 1: Information Sheet

It is important for a risk assessment to include facts about the risks that have been identified. Knowing more about the potential risks to Mount Nittany Medical can help to identify plans or responses to the identified risks. The information provides insight into what some repercussions of not properly dealing with certain risks as well as more information emphasizing why the identified risks are important to address.

"Reports say that hospitals collectively pay upwards of 55.6 billion in medical liability bills that stem from a variety of issues" (Mello, Chandra, Gawande, Studdert 2011)

http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3048809/

"One of these risks that a patient faces is hospital-acquired pneumonia. This infection can often times be deadly too with a mortality rate ranging from 33%-71%" (Keita-Perse, Gaynes 1996)

http://books.google.com/books?id=8dzLdFEtzIUC&pg=PA50&dq=hospital+acquired+pneumonia+mortality+rates&hl=en&sa=X&ei=wRciVNj-BI7_yQSc6oLgCQ&ved=0CC0Q6AEwAA#v=onepage&q&f=false

"More than seven million health records in the United States were affected by data breaches in 2013, an increase of 137% over the previous year."

"There have also been 804 breaches of health information affecting nearly 30 million patient health records reported to the secretary of Health and Human Services, as required by law." (Durbin 2014)

http://search.proquest.com.ezaccess.libraries.psu.edu/docview/1531083682?pq-origsite=summon

"Each year an estimated 5% are misdiagnosed based on currently available evidence." (Singh 2014)

"5% error rate means that more than 12 million adults are misdiagnosed every year, and our study may understate the magnitude." (Singh 2014)

http://search.proquest.com.ezaccess.libraries.psu.edu/docview/1531083682?pq-origsite=summon

Attachment 2: Structured Analytic Results

It is important to generate as many ideas as possible when identifying risks because you so not forget a risk that could potentially happen because if it does, you will not have a plan for it and it could thus deal a crippling blow. Below, are lists with ideas generated using two forms of thinking: divergent and convergent. Divergent is basically saying whatever comes to mind without thinking too much in depth about it. Convergent is the opposite and involves thinking more critically about each one to ensure that the risk being examined is related to the point of view being focused on in this assessment. The divergent results are obviously much longer because they encompass a wide variety of potential risks that a patient could face. The convergent list is much shorter because the team identified three of the risks from the divergent results and used them because these were considered to be the most feasible risks a patient could face.

Patient Hazards at Mount Nittany Medical Center

Divergent Results

- Fire
- Catching pneumonia
- Machine Failure
- Slip
- Incorrect diagnosis
- Cyber-attack
- Hurricane
- Earthquake
- Tornado
- Power Outage

Convergent Results

1. Catching Pneumonia
    - Prevalent in hospitals
    - Very contagious
    - Can be deadly
2. Cyber-attack
    - More of a threat today than before
    - Patient records can be compromised
    - Sensitive information in the wrong hands
3. Incorrect Diagnosis
    - Can be deadly
    - Cost hospitals a lot of money in liability
    - Easily preventable

Attachment 3: Threat Analysis

Table 2 maps out the three main threats that have been identified to be most dangerous to an admitted patient at Mount Nittany Medical Center. The table lists each threat, whether or not the motivation behind said threats are intentional or unintentional, and the action the threat could turn into.

Threat	Motivation	Action
Catching pneumonia while admitted in the hospital	Unintentional spread of infection	Could spread throughout the hospital
Cyber-attack on patient's personal records	Intentionally stealing very sensitive information for some sort of gain	Infiltrating Mt. Nittany's network and stealing the records
Incorrect Diagnosis	Unintentional on the doctor's part	Could put the patient's life in danger

Table 2- Analysis of each threat

Attachment 4: Vulnerability Analysis

Table 3 shows the vulnerabilities that Mount Nittany could potentially have. Each source next to the threats indicates who would be responsible for the vulnerability mentioned. After those two, the action column then explains what could happen if the vulnerability was exploited or manifested itself.

Vulnerability	Source	Action
Lapses in hospital sanitation and doctor protocols	Ventilators and rooms that were not properly sanitized	Pneumonia spreading rapidly throughout the admitted patients
Openings in network security	Unguarded backdoors in the network security perimeter	An unauthorized user could expose the network security flaws and steal patient records
Misdiagnosing a patient	Mt. Nittany doctors	A patient could be treated incorrectly and put their life in jeopardy

Table 3 – Analyzing each vulnerability associated with the risks

Attachment 5: Risk Scenario Likelihood

Table 4 lays out the three risks being examined in this assessment and how likely they are to happen to affect an admitted patient at Mount Nittany Medical Center.

Risk Scenario	Likelihood
Catching pneumonia while admitted in the hospital	Medium
Exposure of patient's personal records due to a cyber-attack	Low
Incorrect diagnosis of the patient	Medium

Table 4 - Assessing the likelihood of the three risks

Attachment 6: Risk Scenario Impact

Table 5 is building off of the risk scenario likelihood. Now that the likelihood of each risk is known, it is important to assess what the impact would be if the risk were to occur.

Risk Scenario	Threat/Vulnerability	Impact
Catching Pneumonia while admitted in the hospital for other illnesses or treatments	Weaker immune system of the patient making them more likely to contract pneumonia	Medium
Cyber-attack on patient's personal records	Insufficient security of Mt. Nittany Medical's information system	Medium
Incorrect diagnosis of the patient	Incorrect analysis of symptoms and various test results by the doctors/nurse/practitioners	High

Table 5 - Combining the risks with their vulnerabilities and impacts

Attachment 7: Risk Matrix

Table 6 is the risk matrix being utilized to quantify the risks involved. Quantifying the risk involves multiplying the likelihood of threat happening by the impact it would have if it were to occur. This product gives a numerical value for the risk. A range of values was established to determine which values would be considered low, medium, and high. The same was also done for the threat likelihood. In this case for example, a threat likelihood of 1.0 and an impact of 100 would score on the risk matrix while a threat likelihood of 0.25 and an impact of 25 would score low on the risk matrix. The Risk Scale is: Low (0 to 24), Medium (25 to 49), and High (50 to 100).

Threat Likelihood	***Impact***		
	High ***100***	***Medium*** ***50***	***Low*** ***25***
High ***1.0***	100 x 1.0 = 100	50 x 1.0 = 50	25 x 1.0 = 25
Medium ***0.5***	100 x 0.5 = 50	50 x 0.5 = 25	25 x 0.5 = 12.5
Low ***0.25***	100 x 0.25 = 25	50 x 0.25 = 12.5	25 x 0.25 = 6.25

Table 6 - A matrix designed to quantify each risk

Attachment 8: Risk Rating

Table 7 is now actually applying the risk matrix to the Mount Nittany assessment. Now that there is a way to quantify the risks, a likelihood and impact value was assigned to each risk after they were assessed properly. These two scores were then multiplied by one another to generate a risk quantity in which a higher number indicates a higher risk and a lower number indicates a lower risk.

Risk Scenario	Likelihood	Impact	Risk Rating
Catching Pneumonia while admitted in the hospital for other illnesses or treatments	Medium 0.5	Medium 50	Medium 0.5 x 50 = 25
Cyber-attack on patient's personal record	Low 0.25	Medium 50	Low 0.25 x 50 = 12.5
Incorrect diagnosis of the patient	Medium 0.5	High 100	High 0.5 x 100 = 50

Table 7 - Applying the matrix to get a score for each risk

Attachment 9: Summary Table

Table 8 brings everything from the previous tables and organizes the information into one larger table. This makes it much easier to find out all of the information associated with each risk which includes: the scenario, risk rating, recommended control, action priority, required resources, responsible party, and maintenance requirement.

Risk Scenario	Risk Rating	Recommended Control	Action Priority	Required Resources	Responsible Party	Maintenance Requirement
Catching Pneumonia while admitted in the hospital for other illnesses or treatments	25 Medium	Mitigate	Medium	Additional cleaning staff and materials, good hand washing	All Mt. Nittany staff; mostly doctors and custodians	Sanitation protocols of rooms and especially ventilators and doctors keeping patients moving
Cyber-attack on patient's personal record	12.5 Low	Accept	Low	Security software package	Hospital cyber-security personnel	Patch network vulnerabilities and increase network security
Incorrect diagnosis of the patient	50 High	Avoid	High	Additional testing materials	Mt. Nittany doctors	More thorough check ups and testing

Table 8 - Combines all of the information into a single table

GRADING RUBRIC

Peer Reviewer: Assign total points here for composition, contribution, subject knowledge and APA citations. Write specific comments into student's paper.

Section _________

1st Author Name (Print): __________________ 2nd Author Name (Print): __________________

1st Peer Reviewer Name (Print): ________________ 2nd Peer Reviewer Name (Print): ________________

Peer Reviewer Points	Max Possible Points	Instructor Total Points	Item
	25		**Composition** - Business professional writing with no grammatical or spelling errors.
	25		**Contribution -** Improves class learning by providing new information or approach to topic under discussion.
	25		**Subject Knowledge** - Knowledge of course content is illustrated by integrating concepts into the essay. Does it appear that you know what you are writing about? Are you aware of aspects of this covered in class?
	15		**Captions, References and APA Citations** - Reference to article, book, or magazine where new information or approach is provided, and appropriate citation in text. Must follow APA format!!! • **In-Text Cite:** Includes author/year, sometimes page number • **Reference List:** Each single-spaced with hanging indent, double-space between citations • **Captions:** Tables/ figures must include complete captions with citation
(blank)	**10**		**In-class peer review** - Thorough and complete with specific comments (i.e. NOT "good job" or "great opening") for what has been done well or what *could* be done to improve the paper
(blank)	**100**		**Total** **INSTRUCTOR/LA GRADER INITIALS ________**