The organization we are looking at is the heartfelt hospital (made up) from Texas and the risks that they could face. The hospital has created a database which contains their patient details and sensitive information. The information they store ranges from medical history to payment methods. The database is backed up in a second location offsite as well as a digital version with a cloud. Their system is not perfect, and this means that there is the chance of threats occurring.

The first threat is malware which is malicious programs that are sent in hopes of gathering data. Malware can be used to cause problems or steal this information. There is a high probability of a malware attack as they are one of the most common threats. It would also have a high impact as the hospital will also store a person’s social security number which could lead to identity theft.

The second threat is an insider threat where one of the employees of the hospital is stealing information to either be sold or used somewhere else. This threat is not as likely but would have a medium impact as they could leak sensitive information they can access.

The third threat is a denial-of-service which would be a threat that attacks the system and shuts it down or makes it impossible to access. This is done to either hold the system hostage for money or to break the system and cause trouble for the hospital. The probability of this would be medium as it could happen but it not as likely as malware while the threat would be high.

The fourth threat is a natural disaster which could be an earthquake or even a tornado. As the hospital is located within Texas, which is on one end of tornado alley, the probability would be high while the threat impact would be in the middle as the information would be easier to fix as it has the backup but may take time as the building could be damaged, this puts the impact in the middle.

|  |  |  |  |
| --- | --- | --- | --- |
| IMPACT | Low | Medium | High |
| Malware |  |  | X |
| Insider Threat |  | X |  |
| Denial-of-Service |  |  | X |
| Natural Disaster |  | X |  |

|  |  |  |  |
| --- | --- | --- | --- |
| PROBABILITY | 0-30 | 30-60 | 60-95 |
| Malware |  |  | X |
| Insider Threat | X |  |  |
| Denial-of-Service |  | X |  |
| Natural Disaster |  |  | X |

The probability and impact analysis shows that the most likely threat would be malware as it has a big impact. A natural disaster also has a high probability but a lower impact thanks to the hospital setting up backups. The best for the hospital is to provide employee training to help identify threats such as malware and keep important hardware within a safe location like a basement or concrete room to protect against tornadoes.

Citations:

*7 types of cyber security threats*. University of North Dakota Online. (2020, October 2). <https://onlinedegrees.und.edu/blog/types-of-cyber-security-threats/>

ABC News Network. (n.d.). ABC News. <https://abcnews.go.com/Health/cyberattacks-hospitals-growing-threats-patient-safety-experts/story?id=99115898#:~:text=ABC%20News-,The%20number%20of%20attacks%20on%20U.S.%20hospitals%20each%20year%20doubled,the%20American%20Hospital%20Association%20said>.

Mead, N. R., & Woody, C. C. (2017). *Cyber Security Engineering: A practical approach for systems and software assurance*. Addison-Wesley.

*Risk assessment*. Health and Safety Executive Northern Ireland. (2021, November 30). <https://www.hseni.gov.uk/articles/risk-assessment#:~:text=A%20risk%20assessment%20is%20simply,prevent%20injury%20and%20ill%2Dhealth>.

Step 1: Identify the hazards - ROSPA. (n.d.). <https://www.rospa.com/rospaweb/docs/campaigns-fundraising/hse-five-steps-to-risk-assessment.pdf>