**Tyler Carrier**

**Information Security**

**Children’s Hospital NH’s Potential Threats**

**Box #88**

**10/16/18**

Nowadays, information within different companies is always at risk. Companies everywhere are being affected by hackers. Hospitals are in particular danger due to the importance of a fully-functional medical system. When taking a look at Children’s Hospital of New Hampshire, it is safe to say that they are not fully aware of the risks that are at hand. This hospital must take a closer look at their security and buckle down. If the hospital fails to do so, they are at risk of having their information stolen, altered, or deleted.

There is a large number of possible data/information which is at risk in reference to the Children’s Hospital of New Hampshire. However, the information which is most at risk are emails, health records, and operating systems. These three main areas are likely to be targeted by hackers. By getting into a hospital’s email system, the hacker has access to a lot capabilities and information. They are able to pose as worker within the hospital and send out false information to other employees. They are also able to have access to important information involving employees and patients.

If a hacker gets access to health records, then the hospital is dealing with a long list of potential issues. The biggest issue with this is protection of the patient’s identity. The hospital could face a lot of legal issues in reference to this issue. The last main area that is likely to be targeted is the hospital’s operating systems. A hospital with a faulty operating system is not able to effectively treat their patients. This type of threat will make the hospital essentially ineffective which puts its patient’s at a huge risk.

Aside from hackers, there is one other associated enemy that the Children’s Hospital of New Hampshire could meet- time. The amount of time it takes to remove a threat may not be worth it for the hospital. Just a few hours of a faulty medical system can lead to tampered, important information and possible even death of their patients. A company in Greenfield, Indiana faced this problem in early January of 2018.

The hospital, Hancock Health paid a sum of $55,000 to put an end to a ransomware infection (Osborne). In this predicament, the hospital’s systems were locked under an encryption key and would continue locked until Hancock paid them in the proper number of Bitcoin. The attack was noticed shortly after 9:30 p.m., but at this point, it was too late. The hackers, supposedly based out of Eastern-Europe, had already compromised the hospital’s system. The ransomware which affected the system was known as SamSam ransomware. The goal of this system is to find a vulnerable source and spread to other networks and hardware from there.

The hospital was forced to switch to pen-and-paper documentation until they could get their system up. Hancock unfortunately was forced to pay the ransom in order to get their systems working again. According to sources, “it may have taken days, maybe even weeks to restore order” (Osborne). This period of time is not realistic for a hospital whose patients are in need of immediate care.

Attacks like these are what the Children’s Hospital of New Hampshire need to weary of. This hospital is in need of the utmost security in order to evade attackers especially those of the “ransomware” calibur. No time is able to be wasted when you are dealing with the health and safety of the hospital's patients. If CHNH is aware of these threats and follows the necessary security processes, the hospital will be in a much less vulnerable position when dealing with various types of hackers.

**Work Cited:**

Osborne, Charlie. “US Hospital Pays $55,000 to Hackers after Ransomware Attack.”

ZDNet, ZDNet, 17 Jan. 2018,

www.zdnet.com/article/us-hospital-pays-55000-to-ransomware-operators/.