# Ransomware on New Jersey Health systems

Recently this November New Jersey's Capital Health hospital was a victim of a Ransomware attack. Capital Health operates hospitals in Trenton and Pennington First notice of this attack was recognized when they found many disturbances in their systems. The disturbances caused a lot of network outages confirming that they were not able to get into some appointments and had to reschedule them. At the time of the post in November Capital Health is unaware if any personal data has been collected like social security numbers, medical records etc. but they are doing what they can to find out what it is. A professional in the field Rob D'Ovidio stated that this attack is most likely for financial gain which makes it a ransomware attack. He explains that this attack does have an organized crime group linked to the attack. It is also explained how ransomware attacks are usually when an attacker blocks access to certain files or networks and requests a certain amount of money and when they receive that money they will give them a decryption key so they can unlock the files or the networks(6abc,2023).

To go into further detail about a Ransomware attack.Ransomware is malware that can lock your data on your device but leave the operating system intact. Which is most likely what is happening with the hospitals since they do not want to bluff. Another way a ransomware to happen is almost like a scare tactic where the attacker sends you a pop up that locks your device and says its from a place that has power and you need to send them money because you violated something maybe like the FBI or the CIA and a normal person without much knowledge would be scared and send them the money. That scenario is easier to fix and can be sent to a professional. In the other scenario, the scenario that I think is happening is the files are actually locked and the only way to get them unlocked is by getting a decryption key and that means you have to pay the attacker for the key. I'll explain what a key is in further detail as well. A key is a type of encryption algorithm that keeps people from accessing certain plain text files and anything that an owner doesn't want seen without a key. There are also multiple types of keys, symmetric or asymmetric/public keys. The main difference between the two is that one of them(symmetric keys) is a key that is used to decrypt and encrypt; that means if someone has the key they can decrypt it and encrypt data. The other type of key is an asymmetric key. An asymmetric key has an encryption key that hides the plain text and a decryption key that decrypts the text. If you have one of the keys it can only do one thing and not the other so a decryption key can not encrypt and vice versa. With that being said I believe the attackers are using an asymmetric key that way they can reuse the encryption key with different attacks without someone knowing the algorithm for that encryption. Capital health are victims because the only way to get the data unlocked is by paying the attackers for the decryption key or they would have to pay a very smart

cryptologist. According to a study one way that the malware that is the ransomware is attached to a system is through a phishing attack(Richardson and North 2017).This is another type of cyber attack that is basically a persuasive email or message to someone to get them to click a link. Once the link is clicked then a malware is downloaded to the device infecting the device.Since it is not disclosed on how the attackers got into the systems In the case of Capital health if someone with access to important files and information clicked a link from an email. The attacker would get access into it as well install the malware (sometimes all of this can be done with the first click) then they are free to start with the ransom. That is a vulnerability I like to call human nature. People are curious which is bad for cyber security because if you click the wrong thing you can mess up something with one click and there is no software to stop someone from being curious. That is my guess of what happened to Capital health and that is why it is important to enforce great cybersecurity to places like a hospital because so much sensitive information is there. I found in a journal that even if the ransom money is given in a lot of cases people do not give the decryption key to the victims and that could be to reuse the encryption  and so none else has the decryption. The journal also mentions that in the future that might happen less frequently being that if the trend continues then companies will stop giving money. In that situation it is a lose lose for everyone (Richardson and North 2017).

In the case of Capital Health I think that they should take the risk and pay for the chance of getting the decryption key. They have a lot of sensitive information that they hold and in the wrong hands it can get worse in many ways. Once they get out of that they should upgrade all software that they already have. In my opinion all of their staff should also get randomly tested on basic cybersecurity precautions. It is so easy to make a mistake because all it takes is one click. When people are at work they tend to get bored and start looking at things or emails. Knowing what is at risk can not stop everyone but it can prevent the majority. Another way to protect from ransomware attacks is possibly having offline backups in a separate location. This way if data is encrypted and there is no access to the online data you still have something in case you never are able to get it back again. Every company should have this in their security policy. It's just another plan that keeps you from having further problems in the future.

Ransomware attacks are very impactful and are getting more popularized because of how much money can get from it. Think of it like this: if someone obtains the information of medical records or social security number they can get the ransom money or they can sell them on black markets for crypto currency which is not easily tracked. Another issue that can be brung from ransomware is the victims of the information can sue companies especially medical companies for lack of security. It is scary for an everyday person that does not know what is going on to learn that a company that they are associated with has been compromised and now they do not know what of theirs has been given away and they can not do anything about it. This

will demand more security policies within a company which could mean more companies implementing things like lock down browsers or browser monitoring all the time, not allowing other devices on the premises or anything. The reason I go to that extreme is because the source of a lot of ransomware attacks are from a human mistake not a device's mistake. The only way to combat a vulnerability like this is to be more strict and possibly make a job feel terrible but things have to be done if it keeps happening. Companies lose too much money from ransomware attacks and they will not go bankrupt because people are making mistakes. As mentioned before I do agree that once this becomes more popular companies will stop paying attackers if it becomes more of a trend to keep  getting the money without giving a key forcing them to find other ways to have files. All of it will cost money whichever way but no one wants to be compromised. It does not give a business a good look. IT also could impact society in a good way if it keeps rising. It will cause the government to take cyber crime more seriously. Even though it might feel like cyber is old it is still young. Crimes like that are serious and I believe depending on situations should be worth years in prison because of how many lives you can ruin at once. Especially if sensitive information is being sold that can lead to identity theft,fraud and all types of things. Everything starts with the policies implementing better policies and making sure policies are being forced. If policies aren't being met then whoever disobeys them should have some type of consequences.

# Work cited

*Capital Health officials say network outages may be caused by cybersecurity incident. 6abc Philadelphia. (2023, November 29).* *https://6abc.com/capital-health-cybersecurity-outage-network-nj-news/14118250/*

*Information Technology Security incident*. Information Technology Security Incident | Capital Health Hospitals. (n.d.). https://www.capitalhealth.org/information-technology-security-incident

Richardson, R., & North, M. M. (2017). Ransomware: Evolution, mitigation and prevention. *International Management Review*, *13*(1), 10.

Below is the same place where I got the information just with working hyperlinks.

https://6abc.com/capital-health-cybersecurity-outage-network-nj-news/14118250/

https://www.capitalhealth.org/information-technology-security-incident

https://digitalcommons.kennesaw.edu/cgi/viewcontent.cgi?article=5312&context=facpubs