GEORGIA INSTITUTE OF TECHNOLOGY
GROUP 10 – OMS CYBERSECURITY MS
ATLANTA, GA 30332

February 22nd, 2020

MEMORANDUM FOR Hospital Chief Information Officer and Chief Information Security Officer

SUBJECT: Assessment of ransomware and its relevance to hospital cybersecurity

1. **PURPOSE**. The purpose of this memorandum is to outline the threat of ransomware to the hospital's information technology (IT) infrastructure. Memorandum further outlines attack vectors, frequency of attacks in historical terms, and the overall threat assessment to the organization.

2. **RANSOMWARE**. Ransomware is a type of malware which gains access to a victim's system and blocks access to his or her files or the system itself by using encryption. As the name suggests, the ransomware continues blocking access to the files or system until the victim pays a ransom, after which a decryption key is provided to unlock the files (De Groot, 2019).

a. Ransomware attacks delay surgeries, treatments, and force hospitals to revert to paper records to continue normal operations (Eddy, 2020). In some cases, the attacker may also include a time deadline to instill a sense of urgency, after which the encryption will remain permanent (Steadman, 2016).

b. Historically, the frequency of ransomware attacks varies from state to state. California has the highest at 25 attacks since 2016. A tame number, however an "attack" is defined as an incident which affects 500+ patients. The four reported attacks in Georgia affected over 190k patient records. (Bischoff, 2020)

c. The means by which a ransomware attack gains access to a victim network is similar to other forms of malware. Three common vectors include email attachments, messages, and malicious pop-up advertisements. As with other forms of malware, the attacker will attempt to disguise the access vector as legitimate communication. (De Groot, 2019)

(1) An email disguised as legitimate communication may trick the victim into opening a link to a malicious website or downloading and opening an attachment with the ransomware payload. The same methods used to deceive victims with phishing, including more sophisticated spear phishing or whaling attacks, can be used to target specific individuals. (De Groot, 2019)

(2) Similarly, attackers can use either compromised social media accounts or fake accounts, posing as their friends or family, to send messages to victims with ransomware attachments or links to malicious websites. (De Groot, 2019)

(3) Malicious advertisements, such as pop-up advertisements designed to look like trusted software, can be used to manipulate victims into downloading and executing ransomware. (De Groot, 2019)

3. **BUSINESS IMPACT**. Ransomware can significantly impact the hospital's business operations from a financial, medical and legal perspective.

a. Financial. Besides the immediate financial cost of the ransom itself, if paid, there is the also the cost of recovering the system, subsequent post-attack analysis to ensure there was no leak of patient data, and protecting the system against future attacks. There are further financial risks if electronic billing systems are affected (Pope 2016). Nationally, ransomware attacks have cost the healthcare industry approximately $157mil since 2016; the state of Georgia an estimated $3.6mil - $5.6mil and affected over 190k records (Bischoff, 2020).

b. Medical. The digitization of patient data and our reliance on electronic data records and systems with respect to patient care makes hospitals especially vulnerable to the risks of a ransomware attack. A successful attack which blocks access to patient records, schedules, and other data, as well as entire computer and communication systems can severely disrupt patient care, putting patients at risk and lowering the quality of care. (Pope 2016)

c. Legal. As a ransomware attack is considered a data breach, there are legal implications in the United States as patient information could be subject to state and federal privacy laws. If such a breach is deemed to have violated state or federal law, then a public investigation and litigation, including private lawsuits, could follow. Any incurred legal fees or fines would be considered another financial risk to the hospital. (Pope 2016)

4. **SUMMARY**.

a. Ransomware is a leading cause for concern in our medical group and should be addressed. Aside from the protection and security that it would provide to our clients, it would also ensure the hospital's protection through financial assurance, ability to treat patients and defend the hospital's overall reputation. In 2019, Interfaith Medical Center initiated network defense measures which saved over $2mil in possible ransomware damages over a seven year period (Eddy, 2020). Security can be achieved through effective safeguard implementations and developing a security mindset amongst employees.

b. This group's recommendation is to implement an additional cybersecurity policy focusing on the threat of ransomware. With the approval of the CIO and CISO, the undersigned will begin immediately. The policy will serve as supplemental to all cybersecurity policies and procedures currently in effect.

5. Point of contact for this memorandum is the undersigned and can be contacted at distribution list pubp6725_group10@gatech.edu or (404) 555-0001.

WILLIAM R. BUCKLEY III
Cybersecurity Contractor
Group 10 – Georgia Tech

Evan Carrillo

EVAN CARRILLO
Cybersecurity Contractor
Group 10 – Georgia Tech

Gladies Huilin

GLADIES HUILIN
Cybersecurity Contractor
Group 10 – Georgia Tech

Victor M. Carrion

VICTOR M. CARRION
Cybersecurity Contractor
Group 10 – Georgia Tech

REFERENCES

Bischoff, Paul. “Ransomware Attacks on Hospitals & Healthcare Cost $157m since 2016.” *Comparitech*, 11 Feb. 2020, www.comparitech.com/blog/information-security/ransomware-attacks-hospitals-data/.

De Groot, Juliana. “A History of Ransomware Attacks: The Biggest and Worst Ransomware Attacks of All Time.” *Digital Guardian*, 24 Oct. 2019, digitalguardian.com/blog/history-ransomware-attacks-biggest-and-worst-ransomware-attacks-all-time.

Eddy, Nathan. “Ransomware Attacks in 2019 Forced Some Health Systems to Pay Up.” *Healthcare IT News*, 2 Jan. 2020, www.healthcareitnews.com/news/ransomware-attacks-2019-forced-some-health-systems-pay.

Pope, Justin. “Ransomware: Minimizing the Risks.” *Innovations in Clinical Neuroscience*, Matrix Medical Communications, 1 Dec. 2016, ww.ncbi.nlm.nih.gov/pubmed/28210525.

“Ransomware Attacks Have Cost the Healthcare Industry at Least $157 Million Since 2016.” *HIPAA Journal*, 17 Feb. 2020, www.hipaajournal.com/ransomware-attacks-have-cost-the-healthcare-industry-at-least-157-million-since-2016/.

Steadman, Zachary T. “Ransomware and Healthcare Providers.” *Arkansas Lawyer*, vol. 51, no. 4, 2016, p. 20.