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

February 26th, 2020

ORGANIZATIONAL POLICY FOR IMMEDIATE DISTRIBUTION

SUBJECT: Security policy guidelines and procedures pertaining to ransomware

1. **PURPOSE**. The purpose of this organizational policy is to outline a security policy for the hospital's information technology (IT) infrastructure. The policy will set out principles, rules, procedures, standards and guidelines to enhance the hospital's security posture through effective prevention, detection, response and recovery practices.

2. **PREVENT**. Prevention is this hospital's first step in ransomware mitigation. We must focus more on the human element than in the technologically automated prevention. Strong emphasis on training and refreshing employees on what to look for when faced with possible attacks is paramount.

a. *Human Element of Prevention - Training*. There are several variants of ransomware that can infect by bypassing human interaction. However, spam emails and phishing are the major attack vectors of ransomware within the healthcare industry. Certain supplementary training requirements for all employees will be implemented.

(1) *Ransomware Prevention Training*. New employee cybersecurity training will now include ransomware discussion and mitigation. Current employees will also be required to complete the training either in-classroom (scheduled with IT department) or the web-based version which includes a quiz. Certificates are obtained by the IT department prior to new employees gaining active user accounts. The training is valid for 12mo.

(2) *Employee Responsibilities*. Complete training annually. Failure to comply results in user lockout from the network. Should this occur, call the IT department immediately for remediation.

(3) *IT Department Responsibilities*. Facilitate in-classroom training when requested. Create web-based training for opting employees. Create automatic reminders for employees starting at 90 days prior to expiration and routinely thereafter. Ensure workstations with guest accounts are accessible for employees who are locked out and must complete web-based training for account reactivation. Update training annually.

(4) *Endstate*. All hospital employees requiring access to workstations are trained and equipped to identify ransomware attacks. Training is in-depth and avoids jargon. Hospital's risk decreases with a knowledgeable workforce and deters attackers.

b. *Technological Element of Prevention*. Along with the human element, software and best practices for cybersecurity must be enforced. Our current policy already has several safeguards and best practices emplaced in accordance with the NIST model. However, certain supplemental adjustments are necessary. Namely, backing up of essential data, more stringent password criteria, anti-malware updates (remote), regular patching (remote), and more comprehensive user restriction.

(1) *Back-Up*. In a work environment which operates 24/7, backing up data is both difficult to execute and enforce. However, it is essential to ensure limited interruption to operations in the instance

of a ransomware attack. Along with the finance department, IT identifies and purchases a minimum of 400TB of backup storage utilizing a reputable and cloud-based service which backs up most frequently used files via encrypted backup processes.

(2) *Stringent Password Criteria*. Stronger passwords serve an important function in prevention of ransomware. Certain variants of ransomware can activate a specific Trojan whose goal is to crack users' passwords. Should an attacker gain access to a user's account on the hospital's network, it would take seconds to install and activate the scheme. Lengthy and complex passwords can be difficult to remember which can impede an employee's ability to work quickly. The IT and Finance Departments will purchase a secure and automated password management tool made available to all employees for use. This will allow quick access and generation of complex passwords for all hospital staff.

(3) *Anti-Malware and Patching*. In our current system, patches and anti-malware are pushed to users for action. The IT Department will now push all patches, software, and anti-malware updates to workstations remotely. Pushes will be made outside of peak operating hours.

(4) *User Restrictions*. The IT Department maintains and grants all users' rights. During in-processing, department supervisors indicate which systems the employee is required to have access to. Each additional access request will be granted so long as the department supervisor signs the request form and provides adequate justification. These restrictions will be more inconvenient to the staff but will ultimately prevent the spread of malware through the entirety of the hospital's network.

b. Implementation of the above will be phased. Estimated implementation of all preventative measures is 120 days. The IT Department along with the undersigned cybersecurity consultants will ensure training is developed and disseminated and all technological elements of prevention are in place at that time.

3. **DETECT**. The identification and possible attribution of anomalous behavior within client network.

a. Ransomware is one of the most troubling types of malicious software that causes problems for individual users and companies. It is important that actions are taken early in order to minimize or eliminate any damage. There are several steps that can be used effectively to thwart ransomware from taking over computer or network files.

(1) Keep up to date on known ransomware file extensions and have file activity monitoring in place so that there is a current and historical record of file and folder activity on the network.

(2) Note any substantial increase in renamed files. A limited number of files may be renamed through normal network file sharing. Ransomware may result in a sharp increase in file renames as your data gets encrypted.

(3) Set up a sacrificial network share that can send alerts when ransomware is found before it takes over the system. Ransomware typically searches for local files and then moves onto the network. An early drive letter can be set up that comes before the actual drive. This 'dummy drive' can be filled with random files that contain no personal, private, or useful information. Access to the disk will be slowed by putting it behind a router with limited data access. This may slow down the logon process for all users but the delay may also provide additional time to shut down any machines before they get

infected with ransomware in the event of an attack. Alerts can also be set up if specific files are accessed. This could provide an early warning that the computer or system has been accessed.

(4) Systems should be updated with exploit detection features. Exploit kits are often used to get ransomware onto a client through spam or compromised websites. Two common exploit kits (EK) used are Neutrino EK and the Angler EK. Check to see if the network security monitoring systems are up to date and are able to detect these and other exploit kits.

(5) Use client based anti-ransomware agents. Antivirus companies like MalwareBytes have software applications to address ransomware. These run in the background and attempt to thwart malicious software like ransomware from encrypting user data. Since ransomware may also attempt to edit the computer registry, text strings of the registry are monitored for any changes. Each client device will need to have anti-ransomware installed in order for this method to be effective. Newer research attempts to look for early entry indications of malware. Ransomware may attempt to install smaller applications prior to installing the main application. Once these smaller malware applications are detected, computer systems can be shut down and thereby minimize any damage to the system or network. Individual users should not install anti-ransomware software on their own device. There is a risk that users could install the incorrect software or not install it correctly and this will leave the system vulnerable.

4. **RESPOND**. Build Incident Response (IR) team and Standard Operating Procedures (SOPs) that will set the foundation on expected behavior in the event of a ransomware attack.

a. *Build an IR team.* Select key personnel who will be responsible for actionable response during critical system errors. This must include employees who manage critical infrastructure to include IT support, network engineers, domain administrators, system engineers, and an IR project manager or team lead. For each role within the IR team, identify a primary and secondary member who can effectively fill the responsibility. The IR team lead or project manager will guide the response team throughout a ransomware attack. The IR team lead should be familiar with all facets of the network infrastructure and everyone’s work role responsibility.

b. *Develop an SOP and response rate Service Level Agreement (SLA).* The SOP will detail circumstantial events, such as variants of ransomware attacks, and define the expected actions to be taken by each member of the IR team. Per each hypothetical ransomware attack, the individual work role will describe if and how all actions should be taken in response to the malware. In congruence with the SLA, the SOP must include expected response times for each possible ransomware attack and each member of the IR team. These time frames will be measured from initial response to a cyber-detection and completion times taken against a specific threat.

c. *Ensure effectiveness of SOP and IR Team.* The IR team lead will certify that all members are aware of their individual responsibilities during a time of crisis. Through tabletop exercises and simulated threats, the SOP can be validated for each ransomware attack. Each member of the team can provide feedback and improvement suggestions for their individual action items. Within the tabletop exercises, create alternative scenarios where the secondary members must respond to ransomware attacks. Following review of SOP and complete team proficiency, additional preparation can be done through internal risk assessments or soliciting a professional penetration testing / vulnerability service provider.

d. *Audit and Review*. Conduct regular review of the SOP on a quarterly basis or if there are any major changes to the technology or infrastructure. Provide routine awareness training to critical IR team members and develop an onboarding guide for transitioning employees into the IR team. Continual training of IR primary and secondary members, SOP reviews and routine tabletop exercises will ensure the preparedness and effectiveness of an incident response to a ransomware attack.

5. **RECOVERY/REMEDIATION.** The recovery and remediation policies following a ransomware attack.

a. *Conduct and validate regular backups.* To maintain the availability and integrity of the service against ransomware attacks. Data backup will be taken weekly to retain up-to-date backups and maintain a distance far enough to escape from any damages or attacks. The backup will be tested bi-weekly to ensure the quality, availability and usability of the data backup resources in case of failures, disasters or attacks. Retention schedules will be adhered to for all business information.

b. *Provide System Restore Points.* System Restore points will be enabled on all network computers that are a part of the hospital's organization. These restore points will enable the opportunity to revert infected machines to a period of completely functionality before becoming infected.

c. *Infection Understanding and Remediation.* Following a ransomware attack, it is critical to understand all aspects of an infection to include the access vector, propagation methods and persistence mechanisms. Considering that an infection might have been in the system for an extended period of time before activation, it is important to conduct extensive historical analysis and understand the complexity of the ransomware attack. The malware needs to be identified to understand the impact and perform the system restoration to a previous state before the date of the attack.

6. **SUMMARY**. Incident response begins with the preparation and continual improvements of current security policies. Through effective implementation, routine awareness training and adherence to an established SOP, the hospital and its incident response team will be adequately equipped for a multitude of potential ransomware attacks.

7. Point of contact for this organizational policy 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
Cybersecurity Contractor
Group 10 – Georgia Tech

ORGANIZATIONAL POLICY for Hospital Chief Information Officer and Chief Information Security Officer
SUBJECT: Security policy guidance and procedures pertaining to ransomware

REFERENCES

Chung, Marcus. “Why Employees Matter in the Fight against Ransomware.” *Computer Fraud & Security*, vol. 2019, no. 8, 2019, pp. 8–11., doi:10.1016/S1361-3723(19)30084-3.

Dargin, Mark. “How to Protect Your Network from Ransomware Attacks.” *Network World*, IDG Communications, Inc., 23 Aug. 2017, www.networkworld.com/article/3218708/how-to-protect-your-network-from-ransomware-attacks.html.

Delaney, Darragh. “5 Methods For Detecting Ransomware Activity.” *NetFort*, 20 Feb. 2019, www.netfort.com/blog/methods-for-detecting-ransomware-activity/.

Kelpsas, Bruno, and Adam Nelson. “Ransomware in Hospitals: What Providers Will Inevitably Face When Attacked.” *The Journal of Medical Practice Management : MPM*, vol. 32, no. 1, 2016, pp. 67–70.

O'Dowd, Elizabeth. “5 Essential Steps for Healthcare Cloud Data Migration.” *HITInfrastructure*, Xtelligent Healthcare Media, LLC, 4 Nov. 2016, hitinfrastructure.com/news/5-essential-steps-for-healthcare-cloud-data-migration.

O'Dowd, Elizabeth. “Planning for Data Backup, Recovery in Health IT Infrastructure.” *HITInfrastructure*, Xtelligent Healthcare Media, LLC, 18 Dec. 2019, hitinfrastructure.com/features/planning-for-data-backup-recovery-in-health-it-infrastructure.

Pope, Justin. “Ransomware: Minimizing the Risks.” *Innovations in Clinical Neuroscience* vol. 13,11-12 37-40. 1 Dec. 2016

“Ransomware: Facts, Threats, and Countermeasures.” *CIS*, 27 Sept. 2019, www.cisecurity.org/blog/ransomware-facts-threats-and-countermeasures/.

Sessions, Lynn. "Ransomware Targets Healthcare Industry." *Mondaq Business Briefing*, 14 Apr. 2016. *Gale General OneFile*, https://link.gale.com/apps/doc/A449462039/ITOF?u=gainstoftech&sid=ITOF&xid=278b3f4b.

Thomas B. Slayton (2018) Ransomware: The Virus Attacking the Healthcare Industry, *Journal of Legal Medicine*, 38:2, 287-311, DOI: 10.1080/01947648.2018.1473186