Ransomware:
Prevention and Coping

Published June 6, 2016

Disclaimer: Destinations Consulting is neither an expert on Ransomware nor offers services to manage IT security. This article is provided as a service for educational purposes only.

Introduction

If you haven't been thinking about Ransomware, you should. It's been thinking about you. According to the Symantec Corporation, Ransomware is up 35% over last year. This year, a Florida ophthalmology practice identified a breach of PHI via a third-party company this year affecting as many as 87,000 patients. In March, two hospitals were attacked by malware. Both hospitals recovered quickly without divulging any PHI, but the attack greatly affected their daily operations. Last year, the FBI released a public announcement stating they had received 992 CryptoWall-related complaints between April 2014 and June 2015, with ransoms totaling over $18 million. These attacks aren't going away or slowing down, they're increasing each year, and most importantly, they're evolving.

What is Ransomware?

Ransomware is a type of software that installs itself onto a computer or system of computers with the intent of either encrypting the computer system or stealing information from it. Typically, the program is written and then sold online to one or many organizations on the black market, leaving it totally untraceable. The software is usually installed by clicking a link on a website or email, but hackers have become more sophisticated recently; new forms of Ransomware look specifically for a hole in security patches. Once the Ransomware is installed, it will prompt the user to pay an untraceable ransom to the hacker in BitCoin to receive a key to decrypt the files.

Prevention

The most important tool you have in fighting against this virtual crime is staff education. Your IT company should be able to provide Security Awareness Training for your business, but if they can't there are other resources available through the Office for Civil Rights and third party companies. Ensure that every person who has access to your computer systems knows what to avoid when opening links in their emails or on websites.

Maintaining current versions of all anti-malware and anti-spam software on ALL devices is critical — this includes tablets, phones, and any equipment that has an internet connection. Convert your mapped drives to UNC; while this may not prevent the attack, it can localize the attack and might be able to keep it from accessing all of your files.

Regularly backup your system, either on a physical drive that's not connected to your system or in the cloud. Backing up your files is crucial to surviving a malware attack of any kind. In the event of ransomware, with a recent backup a practice can avoid costly delays by restoring their system to the backup, eliminating the need to pay the ransom. The frequency of backing up varies from practice to practice. Can you afford to lose a day, a week, or a month of data?

Have a Plan for When, not If

Working closely with your IT team to develop a plan is the best insurance you can have against a Ransomware attack. It should include, but not be limited to, these things:

- Know who is responsible for heading the response, in-office and at your IT company. Make sure that staff knows who to contact as well.
- Contingency Plan - all offices are required to have one to be HIPPA compliant.
- Disaster Relief Plan - a document outlining the steps to take, not stored in your system.
- Develop a method to move to paper charts without too much of a disruption of patient care for each department. You need to know which pieces of equipment are connected to the system and which aren't in the case of an attack, so you know what services you can offer during an exam and which you cannot.
- If and how much you are willing to pay in the case of a ransom?
- How long you can be offline and how to maintain normal business operations without access to your computer system?
- Know when your last backup was and how to access it!
- Know the steps to take if PHI is compromised and how to report a breach.

Resources:

1. FBI Ransomware Pamphlet {https://www.fbi.gov/about-us/investigate/cyber/ransomware-brochure}
2. Incidents of Ransomware on the Rise {https://www.fbi.gov/news/stories/2016/april/incidents-of-ransomware-on-the-rise/incidents-of-ransomware-on-the-rise}
3. Compulink Advantage - Converting Mapped Drives to UNC {http://client.compulinkadvantage.com/wp-content/uploads/UNC_Mapping.pdf}
4. healthit.gov Games on Contingency Plans and Security {https://www.healthit.gov/providers-professionals/privacy-security-training-games}
5. 10 Best Practices for the Small Healthcare Environment {link: https://www.healthit.gov/sites/default/files/basic-security-for-the-small-healthcare-practice-checklists.pdf}