Protecting Yourself from Ransomware

And should you become a victim, here's how to recover.

BY MICHAEL L. BRODY, DPM

Ransomware is a type of malware (malicious software) that denies you access to your data by encrypting the data. The hackers who wrote the malware then ask for a ransom to allow you access to your own data. Paying the ransom may or may not get you access to it. Healthcare has become increasingly vulnerable to ransomware, and one of the most recent high profile ransomware events is the Wannacry attack that disabled tens of thousands of computers and crippled the National Health Service in Great Britain.

It is said that the best defense is a good offense, and this is true for protecting yourself against ransomware. Let's take a look at the history of the Wannacry attack. There was a security flaw in Windows that was known to the NSA. This flaw is known as Eternal Blue. This vulnerability was used by the NSA to monitor computers, but NSA was hacked and the existence of the vulnerability became publicly known. The Wannacry virus took advantage of this particular vulnerability.

As soon as the existence of the vulnerability was leaked, NSA issued a security advisory so that the 'white hats', the people who write antivirus software and security patches for the public, were aware of the flaw. Microsoft released an urgent patch in mid-March to fix the vulnerability and all computers that had the patch installed were protected from Wannacry. Many antivirus developers updated their programs to protect against the vulnerability being exploited and even more computers were protected from Wannacry. Computers and devices that were not patched or protected were at risk of being infected by it. The virus infected 48 UK National Health Service trusts, FedEx, Telefonica, Renault and Nissan car manufacturing plants, U.S. universities, Russian governments, and Chinese ATMs, among many other systems across 150 countries.

In this case, good practices, keeping your computer up-to-date with patches and keeping your antivirus software up-to-date would have effectively protected you from Wannacry as long as you were not using Windows XP.

Wannacry is but one of many types of malware that can infect your computer. Any of these forms of malware can encrypt, corrupt, erase, or even steal your data. It is clear that it is in your best interest to protect yourself from these malicious programs. What steps can you take to minimize the chance of your computer becoming infected?

Install antivirus software and set the software to automatically install updates from the manufacturer.

1) Set your computer to do automatic updates of the operating system. This involves a few clicks and you can arrange for your computer to auto update during 'off' hours to make sure you always have the most up-to-date security patches installed.

2) Install antivirus software and set the software to automatically install updates from the manufacturer. Make sure to keep your subscription up-to-date, make sure the antivirus software monitors your computer, your Internet connection, and your email.

3) Make sure your peripherals, routers, and switches are kept up-to-

Continued on page 40

Ransomware *(from page 39)*

date. These devices sit between our computer networks and the Internet. They have built in software known as firmware. The firmware can be updated to help to keep your network protected.

4) Make sure you keep the programs on your computer up-to-date with the latest versions to prevent hackers from taking advantage of vulnerabilities in those programs. This includes programs such as Adobe, Flash, Silverlight, and other applications that are incorporated into your web browser as well as your web browser (Firefox, Google, Safari, etc.).

5) Make sure your peripherals are properly configured to protect your computers. Each of these devices comes with a 'default' username and password that can be used to configure security. The first thing you should do is change these default values. You then want to shut off all services and ports that you do not need and you want to configure your devices to only allow access to your network through secure ports, preferably using a virtual private network.

6) Prevent your staff from accessing private email using your practice computers either by implementing technology (usually features on your router) or by implementing work rules your staff needs to follow. Opening email attachments is one of the more common methods of getting a malware infection.

7) Make sure all patient data on your computers has been encrypted by you. Encryption is the process of scrambling information and without the decryption key, you cannot use the data. When you encrypt the data, you know the encryption key and you can get your data. When the ransomware encrypts the data, you do NOT have the encryption key and you cannot get your data. If your data is encrypted, and a virus allows somebody to steal your data, the information they get is encrypted and you do not have a HIPAA breach.

Even with all of these preventive measures, computers are still infected with malware. There are steps you can take in advance to allow you to recover from a disaster such as ransomware. These steps are known as your disaster recovery plan. A disaster recovery plan is a vital part of your HIPAA Security Plan.

Let's think about what you would need to do if you completely lost your office to a disaster such as a fire. Here are the steps you might follow:

1) Replace your computers and network equipment

2) Re-install the programs on your computers

3) Recover your data from your most recent back-up

In the case of ransomware or other malware, you may only need to 'wipe' the computers and start from scratch rather than purchase new hardware.

This sounds simple and for the most part it is, but being ready to go through these steps requires some pre-planning. Let's start with step 3—Recovering your data. In order to recover your data, you need to have a copy of your data to use. You need to perform regular back-ups of your data. This data is more than just your EMR system. You also need to have any digital imaging systems such as digital x-ray systems, and you need to have your practice management system and all other systems that have critical information backed up regularly. The back-up needs to be offsite and not connected to your computers. If your office were to burn down, and your back disk were to be next to your computer, then your back-up burned down also. If you get ransomware, and your back-up disk is connected to your computer, the ransomware is on your back-up disk also. You need to have off-site back-up. This can be accomplished by simply bringing the back-up disk home each evening or using an online offsite back-up service. You also need to 'test' your back-up regularly and make sure that if you need it, you can use it. The best way to test your back-up is to reach out to your vendors and ask them to do a test restore of your data and make sure they can restore the data. NEVER test your back-up by restoring to your live system. If the restore fails or the back-up is corrupted, you have just destroyed your 'live' data and you do not have a back-up to use for recovery.

Moving backwards to step 2, you need to maintain a relationship with your vendor. You will need to reach out to them to assist you in re-installing all software that you need to 'use' your data. Usually this involves simply keeping your service agreement up-to-date. Step 1 is to a certain degree the easiest; go to your supplier and purchase new computers.

As long as you are prepared with back-ups that you can restore from, vendors who can re-install the programs and help you restore your data, and somewhere where you can go to purchase new computers, you can recover from a disaster. In the case of ransomware or other malware, you may only need to 'wipe' the computers and start from scratch rather than purchase new hardware.

Each of the steps outlined in this article are part of your HIPAA security program. In the case of malware, ransomware, or a full disaster such as an office burning down, you can be in a position to recover all of your data and have continuity of your business and practice. **PM**

Dr. Michael Brody has presented webinars for the e-Health initiative, (www.ehealthinitiative.org/) and is active in the EMR workgroup of the New York E Health Collaborative (www.nyehealth.org/). He has provided consulting services to physicians for the implementation of EHR software and to EHR vendors to assist in making their products more compatible with CCHIT and HIPAA guidelines. Dr. Brody is a member of AAPPM.