FEDERAL TRADE COMMISSION
CONSUMER INFORMATION
consumer.ftc.gov

Ransomware worries? Keep up to date.

May 15, 2017
by Nat Wood
Associate Director, Consumer & Business Education, FTC

You've probably heard about the ransomware attack affecting organizations' computer systems around the world. It seems to affect server software on organizations' networked computers. But ransomware can attack anybody's computer, so now is a good time to update your own operating system and other software. And then keep them up-to-date.

The ransomware in the news now is known as WannaCry or WannaCrypt. It locks users out of their systems until they pay the crooks who installed it. This ransomware takes advantage of a security hole in Windows server software that can be closed by an update from Microsoft. Many of the organizations affected by the ransomware had not installed the software update.

Even if you only have one computer, download security updates as soon as they're available – no matter what operating system you use. Hackers are constantly looking for security gaps, and companies try to close those gaps as soon as they are discovered. So it's important to download updates right away. Most operating systems have a setting to download and install security updates automatically. Use it. And install updates for your other software, including apps.

If you use old software that doesn't update automatically, set up a regular schedule to go to the company's website and download and install updates yourself. It's wise to check at least weekly.

In addition to keeping software up to date, here are a couple of other things you can do to prepare for a ransomware attack:

- **Back up your important files.** From tax forms to family photos, make it part of your routine to back up files often on your computers and mobile devices. When you're done, log out of the cloud and unplug external hard drives so hackers can't encrypt and lock your back-ups, too.
- **Think twice before clicking on links or downloading attachments and apps.** Ransomware often is downloaded through phishing emails. You also can get ransomware from visiting a compromised site or through malicious online ads.

Blog Topics: Privacy, Identity & Online Security

However, even if the PHI is encrypted in accordance with the HHS guidance, additional analysis may still be required to ensure that the encryption solution, as implemented, has rendered the affected PHI unreadable, unusable and indecipherable to unauthorized persons. A full disk encryption solution may render the data on a computer system's hard drive unreadable, unusable and indecipherable to unauthorized persons while the computer system (such as a laptop) is powered down. Once the computer system is powered on and the operating system is loaded, however, many full disk encryption solutions will transparently decrypt and encrypt files accessed by the user.

For example, if a laptop encrypted with a full disk encryption solution in a manner consistent with HHS guidance[8] is properly shut down and powered off and then lost or stolen, the data on the laptop would be unreadable, unusable and indecipherable to anyone other than the authenticated user. Because the PHI on the laptop is not "unsecured PHI", a covered entity or business associate need not perform a risk assessment to determine a low probability of compromise or provide breach notification.

However, in contrast to the above example, if the laptop is powered on and in use by an authenticated user, who then performs an action (clicks on a link to a malicious website, opens an attachment from a phishing email, etc.) that infects the laptop with ransomware, there could be a breach of PHI. If full disk encryption is the only encryption solution in use to protect the PHI and if the ransomware accesses the file containing the PHI, the file containing the PHI will be transparently decrypted by the full disk encryption solution and access permitted with the same access levels granted to the user.

Because the file containing the PHI was decrypted and thus "unsecured PHI" at the point in time that the ransomware accessed the file, an impermissible disclosure of PHI was made and a breach is presumed. Under the HIPAA Breach Notification Rule, notification in accordance with 45 CFR 164.404 is required unless the entity can demonstrate a low probability of compromise of the PHI based on the four factor risk assessment (see 45 C.F.R. 164.402(2)).

---

[8] HHS guidance to render unsecured PHI unusable, unreadable or indecipherable to unauthorized individuals indicates that encryption solutions for data-at-rest must be consistent with NISP SP 800-111, *Guide to Storage Encryption Technologies for End User Devices*, in order for encrypted PHI to not be "unsecured PHI". It must be noted, however, that consistency with NIST SP 800-111 requires not only the consideration of an encryption algorithm, but also consideration of additional areas of an encryption solution including encryption methodologies (e.g., full disk, virtual disk/volume, folder/file), cryptographic key management, and pre-boot authentication, where applicable.