NATIONAL
RURAL HEALTH
RESOURCE CENTER

Cybersecurity Threats in Rural America

How to Protect Your Critical Access Hospitals

Joe Wivoda

CIO & HIT Consultant

September 27, 2016

The Center's Purpose

The National Rural Health Resource Center (The Center) is a nonprofit organization dedicated to sustaining and improving health care in rural communities. As the nation's leading technical assistance and knowledge center in rural health, The Center focuses on five core areas:

- Transition to Value and Population Health
- Collaboration and Partnership
- Performance Improvement
- Health Information Technology
- Workforce

Why is this Important?

- According to HHS Office of Civil Rights (OCR), as of September 2016:
  - 168,320,984 patient names have been REPORTED to have been breached
  - 126,000,000 of those breaches are reported as having either hacking or other IT issue being a factor
- Medical records are incredibly valuable!
  - Credit Card number: < $5
  - Social Security Number: <$20
  - Medical Record: Between $100-$1,300

Overview

- Understand the types of cyber threats that exist today
- Review the mechanisms that malware commonly use to infect computers
- Discuss the consequences of a malware attack
- Present some steps that critical access hospitals (CAHs) can take to reduce the risk
- Discuss how to respond to a malware incident
- Discuss a particular type of malware, "Ransomware" and the unique threat it presents

Threat Landscape

- Viruses: Infects files and seeks to replicate itself
- Worms: Standalone malware that replicates itself
- Trojan Horses: Misleads users of its true intent
- Spyware: Tracking software, without consumers knowledge

Threat Landscape

- Adware: Software that delivers advertising, often unwanted
- Scareware: Malicious software that uses social engineering to scare you into doing something
- Ransomware: Software that holds your data hostage, usually with encryption technology

Infection Mechanisms

- Media
  - Floppies, CD-ROM, USB drives, etc.
- Network
  - Poor security on local networks
  - Open ports and flawed services
- Email
  - Attachments, including .doc and .zip
  - Embedded HTML
- Web browser
  - Social engineering
  - Browser flaws
  - Remote code execution

An Example

- Search for information or software in Google
- Of the several sites listed, you select one that has been compromised
- An ad appears that looks like a legitimate error message
- Your files are now being encrypted

Ransomware Example

From https://www.microsoft.com/en-us/security/portal/mmpc/shared/ransomware.aspx

Consequences

- Patient care processes can be disrupted
  - Hospitals have gone on divert
- Business process can be disrupted
  - Months of backlogged bills
- Reputation damage
  - Particularly if there is a reportable breach
- Patient data loss
  - Identity theft
  - Unreimbursed medical care
  - Financial losses for patients

When has a Breach Occurred?

- **ANY** malware event is a security incident and requires an incident response
- Determination of the likelihood of whether protected health information (PHI) was acquired by the attacker
  - Malicious encryption is assumed to mean the data was acquired
- This incident response and investigation is key to breach determination
  - May require third-party experts

Steps CAHs Should Take

- Have good HIPAA policies and practices
  - Risk assessment
  - Incident response
  - System monitoring
- Backups, backups, backups!
  - Good backups are fundamental
  - Need to be verified
  - Offsite storage, but be careful about security

Steps CAHs Should Take

- Install and maintain anti-malware software
  - Centrally managed is best
  - Include Windows Servers, but work with your electronic health record (EHR) vendor
- Keep Windows and browser software up to date
- Sound firewall practices
- Have good downtime procedures and test them
- **Train staff on smart browsing!**

These are all fundamental IT responsibilities that can be a luxury for small IT departments!

The CAH Dilemma

- Complex IT systems
- 50-200 computers
- Limited IT staff
- Massive vulnerability to malware!
- **Need to rely on quality third party vendors**
  - Antivirus
  - Backups
  - Firewall
  - PC management

How to React to a Cyber Event

- Before you can react, you need to be able to identify that there was an event!
  - System monitoring
  - Notifications from antivirus software
  - Firewall notifications
  - End-user notification
- Assemble the right team, quickly
  - May require outside expertise
- If it is a propagating malware (virus, worm, etc.) then consider ways to stop the propagation

How to React to a Cyber Event

- Gather as much information as possible
  - Log files and backups need to be preserved
- Determine whether PHI was acquired
  - How many patient records?
  - What specific information?
- If the event is ransomware, then notification of law enforcement, local and FBI, as well as OCR is recommended
  - See CMS Fact Sheet: Ransomware and HIPAA: https://www.hhs.gov/sites/default/files/RansomwareFactSheet.pdf

Do You Pay or Not?

- Even if you pay, there is no guarantee that you will get the data back
  - You are still required to follow breach notification rule
- Restore of files could take a significantly long time, depending on the size of the data
- In many cases the payment is much less than the cost of lost revenue and possible patient safety concerns

Summary

- Malware will continue to be a threat
- Protecting your facility requires more than good antivirus software
- Good IT practices, including well-tested backups, antivirus software, firewalls, and system monitoring are critical
- End-user training can prevent most malware from spreading
- Most CAHs will need help from outside vendors that do not need to be local

NATIONAL
RURAL HEALTH
RESOURCE CENTER

Joe Wivoda

CIO & HIT Consultant

(218) 262-9100

jwivoda@ruralcenter.org

Get to know us better:
http://www.ruralcenter.org