wednesday webinar

PRESENTED BY PALMETTO CARE CONNECTIONS

Cybersecurity Best Practices in Health Care

Wednesday, January 27, 11am-12pm EST

Presenter:

Jason Cherry, MBA
Director, IS Technology Services
Lexington Medical Center

This webinar is being recorded.

Please mute your phones to eliminate background noises.

The webinar recording and presentation
will be available after the webinar.

PALMETTO CARE CONNECTIONS™
technology. broadband. telehealth.

Cybersecurity Best Practices in Healthcare

Background

- **Lexington Medical Center**
  - 557 bed hospital located in West Columbia, SC
  - New North tower opened in February 2019
  - 7,000+ health care professionals.
  - 70 physician practices
  - 5 community medical and urgent care centers
  - One of the busiest Emergency Departments in South Carolina
- **Jason Cherry**
  - 15 years of Healthcare IT experience
  - Prior to that, 6 years experience in Financial Services IT
  - Team is responsible for all datacenter operations at LexMed – Backup, Network, Server, Storage, Telecom
  - Do NOT have direct Information Security responsibilities, but work closely with a peer Director that does

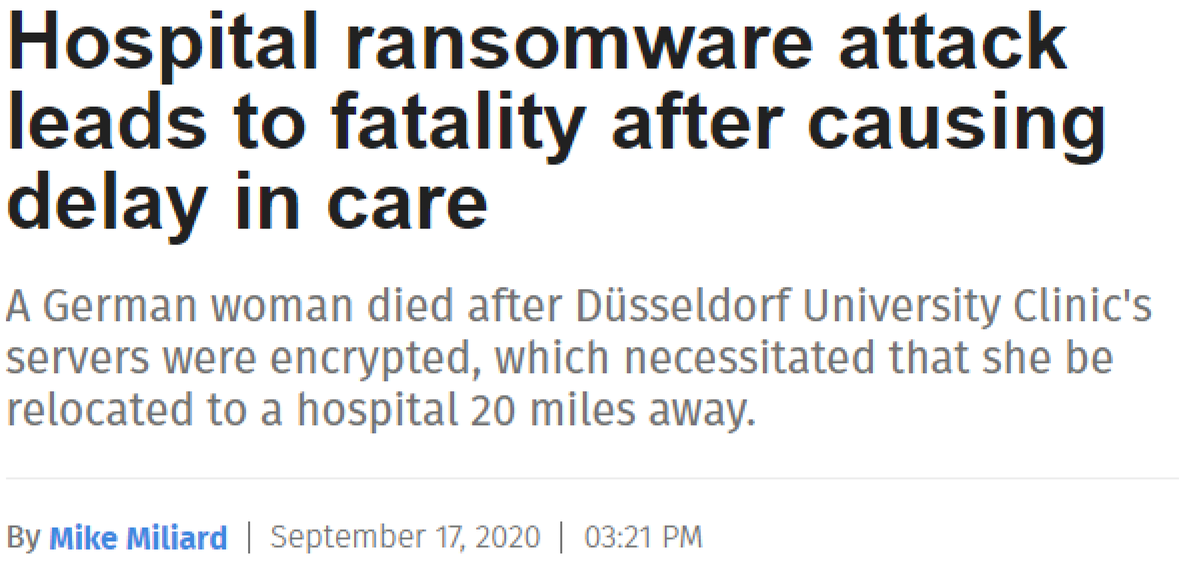
Why Healthcare?

- **Prime Target and Vulnerable for Multiple Reasons**
  - Protected Health Information (PHI) is high value data
  - More IoT/wireless devices that have the potential to be less secure
    - Most often these devices connect to or care for the patient, so they are an excellent entryway into your EMR
  - Patients and their families bring their own devices and expect to connect to wireless
    - This has become an essential part of the patient experience
  - Regulatory bodies that lag behind in approving patches for certain applications
  - Increasing reliance on cloud-based applications. Data is outside your 4 walls.
  - Information systems have become critical in delivering effective and safe patient care

The Impacts of a Breach Are Catastrophic

- **PHI breaches are expensive – fines and credit monitoring services**

- **Ransomware is deadly**
  - Grinds hospital operations to a halt
  - Paper processes are much less efficient and can lead to safety issues
  - Impact can linger for weeks or months
  - Substantial financial impact even if ransom is paid



Hospital ransomware attack leads to fatality after causing delay in care

A German woman died after Düsseldorf University Clinic's servers were encrypted, which necessitated that she be relocated to a hospital 20 miles away.

By **Mike Miliard** | September 17, 2020 | 03:21 PM

How Can My Organization Stay Out of the News?

- **4 Pillars**
  - **Communication**
  - **Documentation**
  - **Education**
  - **Isolation**

Communication

- Get all IT teams actively involved in InfoSec and sharing information frequently
  - Sharing responsibilities helps keep everyone accountable
  - Multiple sets of eyes helps make sure nothing is missed

- Rely on Feds and friends! Several excellent Cybersecurity groups
  - Cybersecurity & Infrastructure Security Agency – www.cisa.gov
  - InfraGard – www.infragard.org
  - Internet Crime and Complaint Center – www.ic3.gov
  - SLED – SC Critical Infrastructure Cybersecurity Program
  - Becker's Hospital Review - https://www.beckershospitalreview.com/cybersecurity.html
  - Health IT Security - https://healthitsecurity.com/

Documentation

- Plan ahead! Document your general response plan and store in a secure location
  - What are your critical applications?
  - What are your most vulnerable/insecure systems?
  - Be part of your Business Continuity plan
  - Review and update **AT LEAST** annually
  - Have an off-network copy

- Practice! Practice! Practice!
  - Test data restores of critical systems from a variety of methods/locations
    - Document any gaps and look for improvements. Be honest!
  - Tabletop drills to test out scenarios and mock events. Prepare for the worst
    - Allows for a much calmer response if an actual event happens. Everyone knows their part

Documentation

- Password policies documented and understood
  - Minimum basic security requirements
  - Required to change on a regular basis
  - Cannot reuse previous # of passwords
  - Elevated privileges should have elevated security requirements

- Account deactivations
  - Have a solid process to deactivate user accounts for people that leave the organization as soon as possible
    - Make sure all access has been revoked when it is supposed to be revoked
    - Have audit logs of all account deactivation work

Documentation

- Patching policies documented and understood
  - Policies for every Operating System that is maintained
  - Maintain a regular cadence of patching to allow for testing while remaining current with security patches
  - Automate patching where you can

- Off cycle/Emergency Patching
  - Have a process documented for ad hoc/off-cycle patching
    - Understand the systems that need to be patched 1st, 2nd, 3rd……….
    - Makes it easier to process patches efficiently in a crisis

- AT LEAST annual audits of your environment to make sure all applicable policies are being followed and enforced

Education

- Get users involved. Make sure they understand the importance
  - Encourage users to report suspicious email no matter how insignificant it may seem
  - Reward users for participating
    - Monthly, random phishing test – users that report the email get a meal ticket
- Invest in Cybersecurity education
  - For users that fail monthly test, a quick video to refresh how to spot a phishing attempt
  - Track metrics for monthly tests and celebrate successes.
    - Helps demonstrate progress and keep everyone accountable
- Tightrope walk between being an alarmist and nonchalant
  - Be transparent to end users, but use non-technical terms

Isolation

- Isolate important systems and only allow minimum necessary communication
  - Focus on critical applications and protecting your organizations most important data
  - Definitely isolate most vulnerable/insecure systems from everything else
  - Monthly, random phishing test – users that report the email get a meal ticket

- Backups and snapshots
  - Make sure backups/snapshots of critical systems are stored in multiple places/datacenters
  - At least one copy should be airgapped/off network/inaccessible by normal means
  - Understand differences between backups and replication
  - Backups are no good if they cannot be restored. Test the process regularly and understand recovery times

- Use 2FA for anything outside your network or your control

Questions?