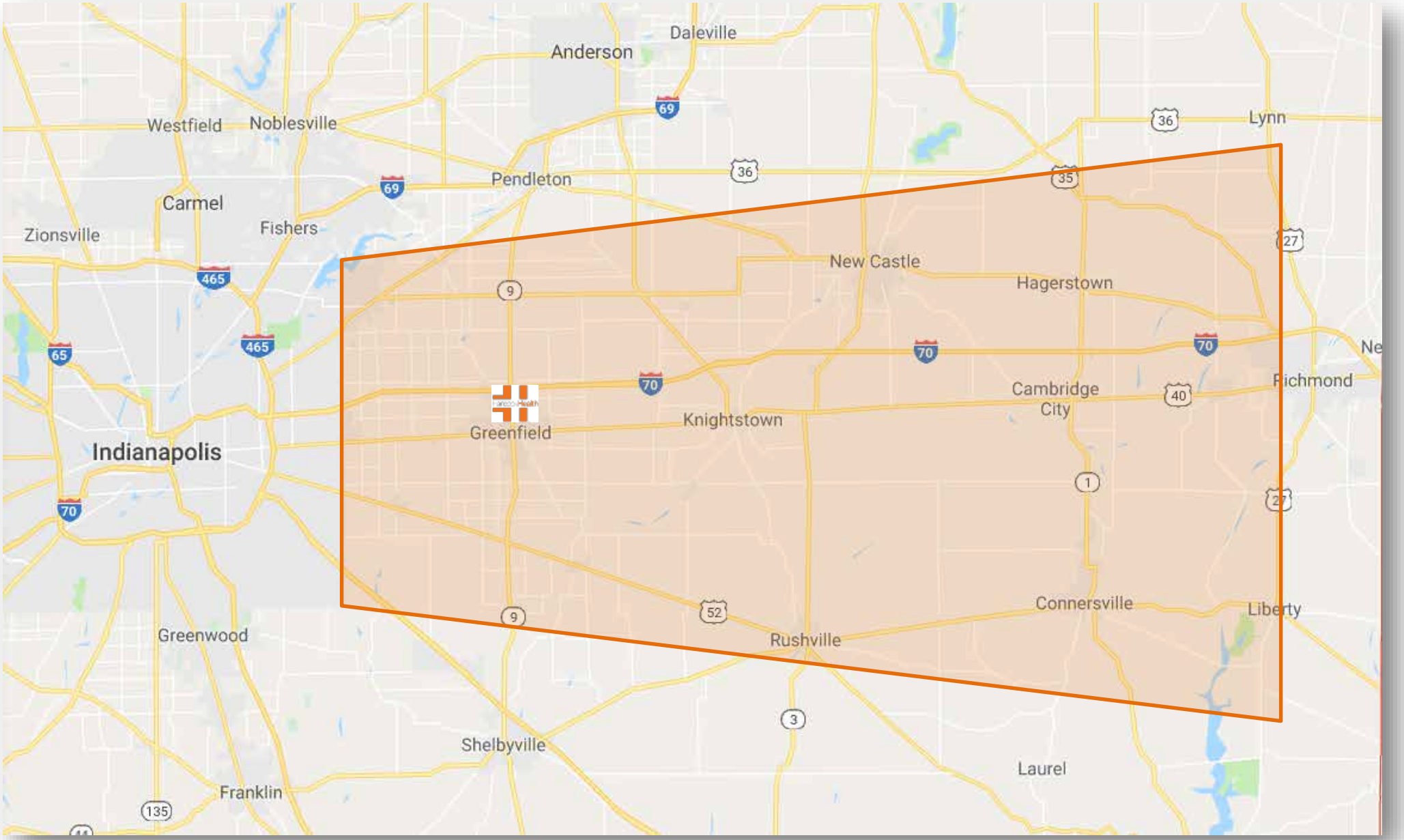
SURVIVING THE "CYBERPOCALYPSE"

Craig Felty
Vice President, Patient Care Services
Hancock Regional Hospital



HancockHealth

Independent health system, $150M annual revenue, 1,200 employees, 150 active medical staff members, 20+ locations including a multi-site, multi-specialty physician practice, two diagnostics centers, cancer center, and two wellness centers, anchored by a 68-bed full service community hospital

Our Time Together

- Pre-incident conditions
- The incident
- The response
- The legal analysis
- Preparing for an incident
- Lessening the likelihood of an incident

HancockHealth

Pre-Incident Conditions

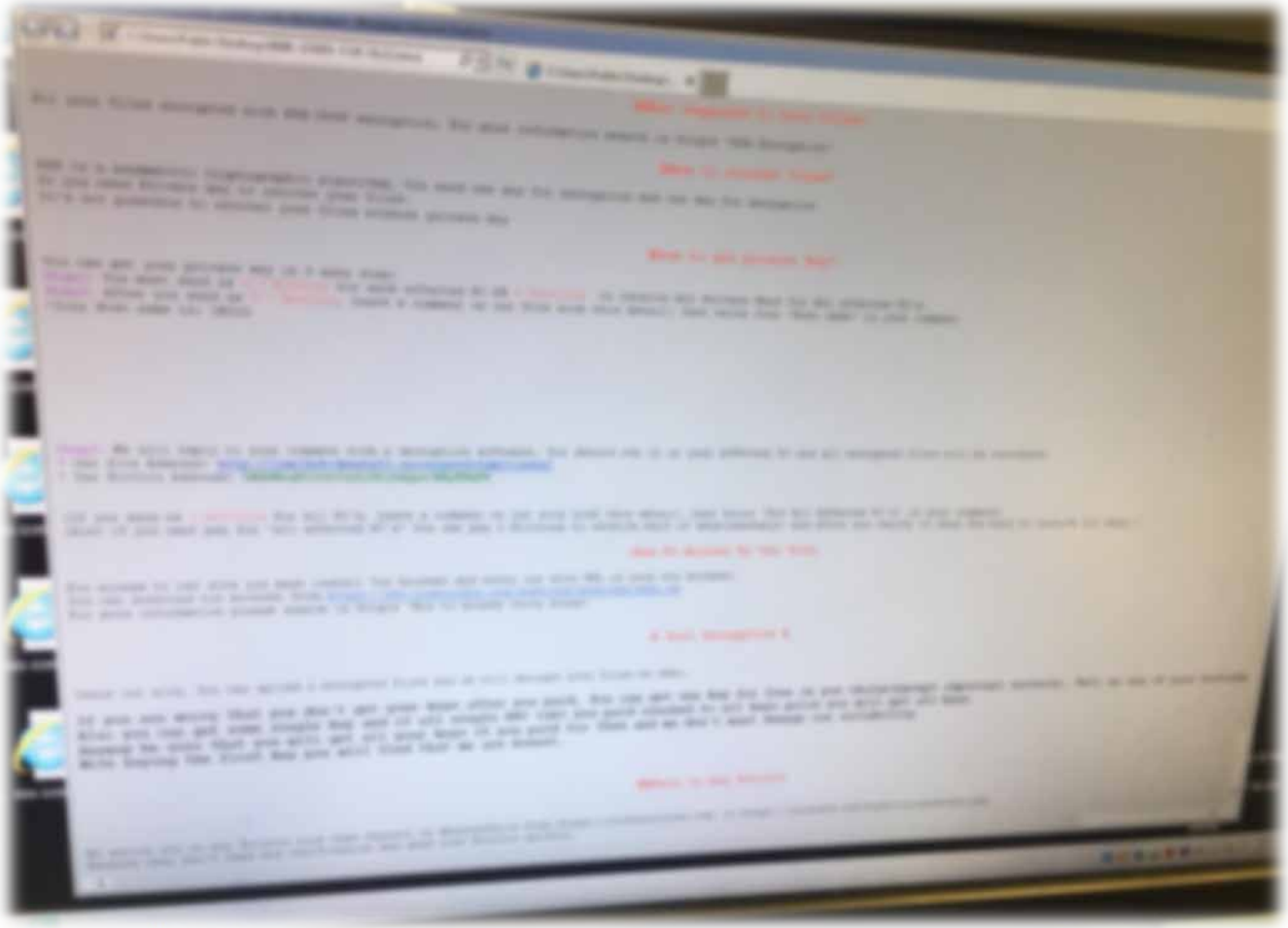
- Most Wired x three
- Comprehensive HIPAA privacy and security program
- Board and C-Suite support for privacy and security
- Area ERs on diversion due to high census of flu patients
- Heading into a holiday weekend
- Inclement weather approaching

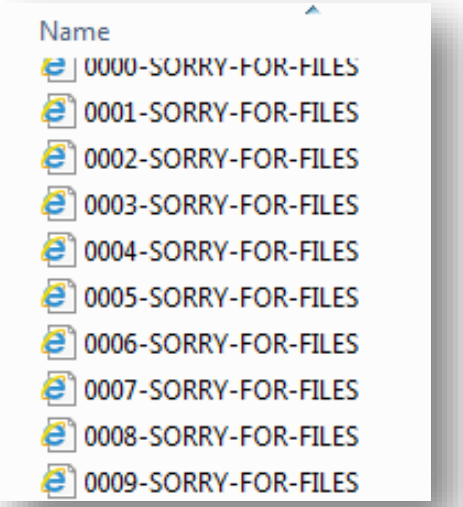
The Incident

- Thursday at 9:30 PM: Messages began appearing on PC screens in the hospital indicating that the system was encrypted with SamSam ransomware and that decryption keys could be purchased with four Bitcoin.
  - One week deadline or data would be encrypted permanently
  - Message included step-by-step instructions for obtaining the decryption keys

HancockHealth

What it Looked Like …





HancockHealth

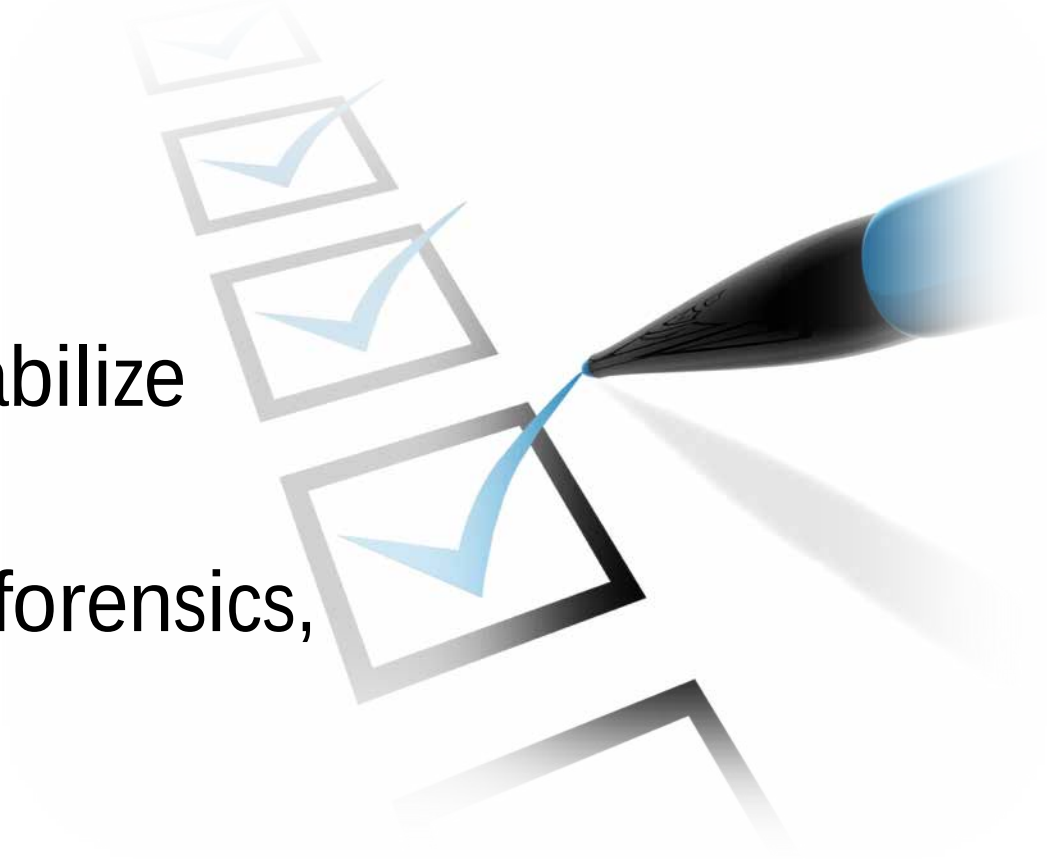
Guiding Principles for the Response

1. Patient safety (always …)
2. Security of patient information
3. Time to restoration

HancockHealth

Response Steps

1. Activate Disaster Response Plan
2. Initiate downtime procedures and stabilize patient care processes
3. Contact key parties (legal counsel, IT forensics, FBI)
4. Initiate IT forensic investigation
5. To pay or not to pay?



HancockHealth

1. Activate Disaster Response Plan

- Immediate shut down of all network and desktop systems
  - Manual process involving more than 1,200 units
  - Signs posted at all facilities noting all computers to remain off
- Incident command center established by executive leadership
  - Non-essential staff called-off
  - Communications by cell phone, text and non-system email

diagnotes® Patient care. Anywhere.

LIVEPROCESS

Board Effect

HancockHealth

2. Downtime Procedures and Patient Care

- Ensured patient-facing equipment unaffected
- Patient care staff moved to paper documentation
- ER diversion only until processes established and stabilized
- Patient care continued throughout the incident:
  - Babies were born, surgeries were completed, patients were treated in ER and admitted, imaging and lab testing was performed … we did what a hospital does every day …

3. Contact Key Parties

- Very early Friday morning: Leadership contacted legal counsel
- Legal counsel engaged an experienced IT forensics firm
  - Will you be able to use your preferred firms?
- Established schedule of calls to occur every two hours
  - Initial call cadence should be frequent, but can become less frequent as needs dictate.
- FBI contacted and included on calls
  - FBI role is advisory and investigative

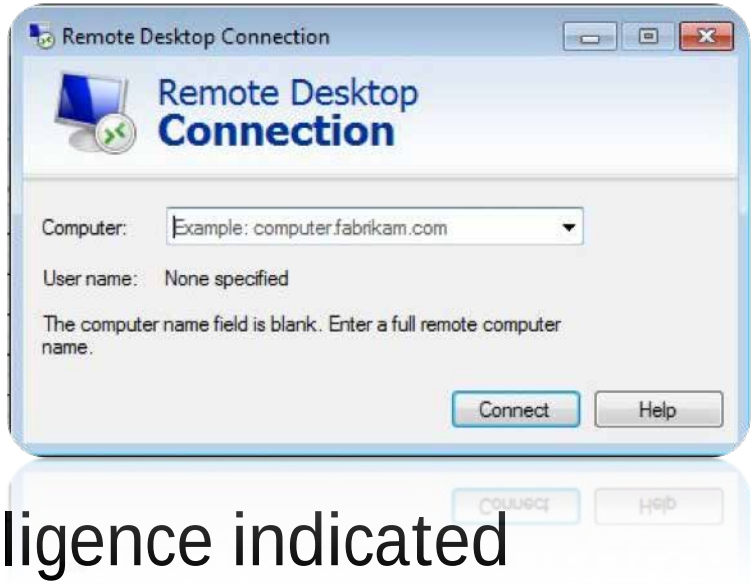
HancockHealth

4. Initiate Forensic Investigation

- Four stages:
  1. Identification
  2. Containment
  3. Eradication
  4. Remediation
- Failure to follow this process could result in incomplete resolution and continuing incident.

Forensic Investigation (cont.)

- Review of logs determined that:
  - Attackers deployed ransomware through a vendor's remote desktop protocol (RDP) access credentials
  - Limited amount of access time
  - No additional accounts created on network
  - No lateral movement within network
  - No evidence of ePHI exfiltration
  - Ransomware was SamSam variant, which intelligence indicated seeks ransom payment only, not data acquisition



5. To Pay or Not to Pay?

- FBI recommends not paying, as a deterrent
- Fact-sensitive determination
  - Do reliable backups of critical data exist?
  - How long will it take to restore from backups?
  - What is the value of time for the affected provider?
- Risks of payment:
  - Make yourself a future target
  - Don't get data back
  - The attackers ask for more money
- Success of business model relies on "integrity" of attackers

To Pay or Not to Pay? (cont.)

- Payment in form of Bitcoin
  - For most, it takes several hours to acquire Bitcoin.
  - Once Bitcoin is acquired, must go on the dark web to make payment to attackers.
    - Must follow instructions precisely
    - Use a secure device to conduct transaction
    - Bitcoin transactions are not instantaneous and can take an hour or more.
    - Then you wait for the attackers to provide the decryption keys

To Pay or Not to Pay? (cont.)

- Decryption keys
  - Could be one key or many keys
  - Decryption process takes time
- Restoring data and bringing systems back online is a slow and deliberate process (much slower???)

HancockHealth

Legal Analysis

- State and federal laws potentially apply
- State laws often focus on risk of identity theft
- HIPAA presumes a breach when Privacy Rule is violated
  - Is all ransomware an unauthorized access/disclosure?
  - Can overcome presumption if able to document that there is a low probability that PHI has been compromised
- Key Factors for ransomware incident:
  - Was ePHI or PII acquired or viewed?
  - Was data availability compromised?

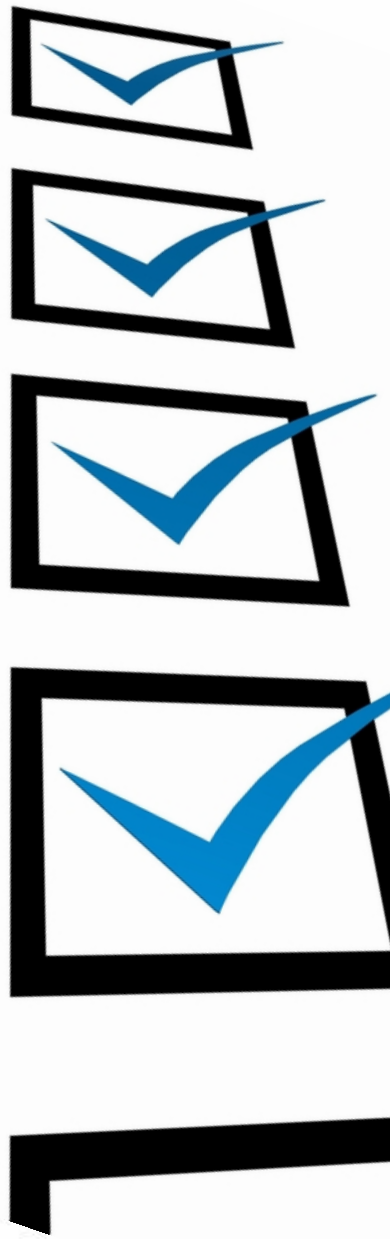
HancockHealth

Preparing for an Incident

- Develop incident response plan
- Characteristics of an effective Incident Response Team:
  - Availability
    - Requires complete dedication to the task at hand
  - Selflessness
    - It's not about you, it is about getting it right. No egos allowed.
  - Delegation
    - Trust your team. You can't do it by yourself.
  - Honesty
    - Truth is integral to this process.

Preparing for an Incident (cont.)

- Practice implementing the response plan (table top exercise).
- Obtain cyberliability insurance.
  - Be sure you can utilize your preferred vendors for legal, forensics, credit monitoring, and mailing
  - Ensure coverage is adequate
- Ensure appropriate liability protections in vendor contracts.
- Enable detailed system and application logging.
- Strong day-to-day organizational dynamics and relationships are fundamental to success (marginal performance in good times means implosion during a crisis …)



Lessening the Likelihood of an Incident

- Conduct enterprise-wide risk analysis
- Develop and implement remediation plan
- Regularly update and patch software and systems
- Implement multi-factor authentication
- Implement a vendor management program

HancockHealth

Lessening Incident Likelihood (cont.)

- Conduct regular workforce training
- Obtain independent third-party penetration testing
- Implement managed security services to monitor IT activity, vulnerabilities and risks

Resolution*

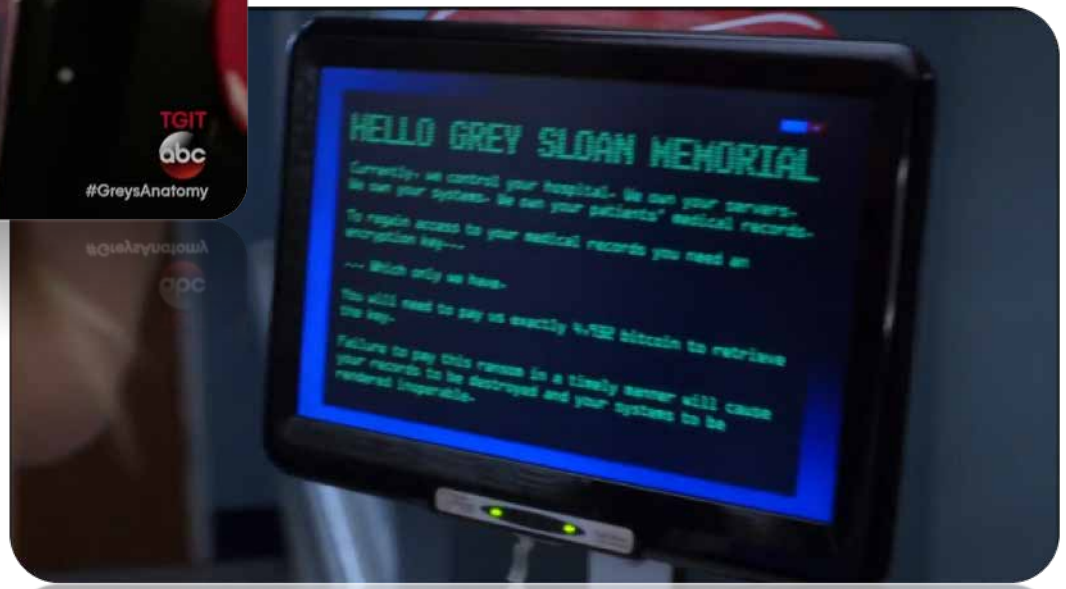
- Thursday
  - 9:30 PM – Cyber-Attack
  - 11:00 PM – all systems shut down,
  - Midnight – Incident Response Team in place
- Friday
  - Early AM – attorneys, IT forensics team in progress
  - Mid-day – Cylance installation in progress
  - Afternoon – Ransom decision made
  - Evening – Bitcoin procured
- Saturday
  - Early AM – decryption keys acquired (i.e. ransom paid – 4 Bitcoin ~$55,000)
  - Mid-morning – file decryption begins
- Sunday
  - Morning
    - Servers & PCs operational
    - Signs removed
  - Early evening – Critical Systems on line
- Monday
  - Most systems operational
- Within a few weeks all systems operational
  - Some Outlook calendar files unrecoverable…

** Regular updates to employees, medical staff, and Board of Trustees throughout*

HancockHealth

Expect the Unexpected …

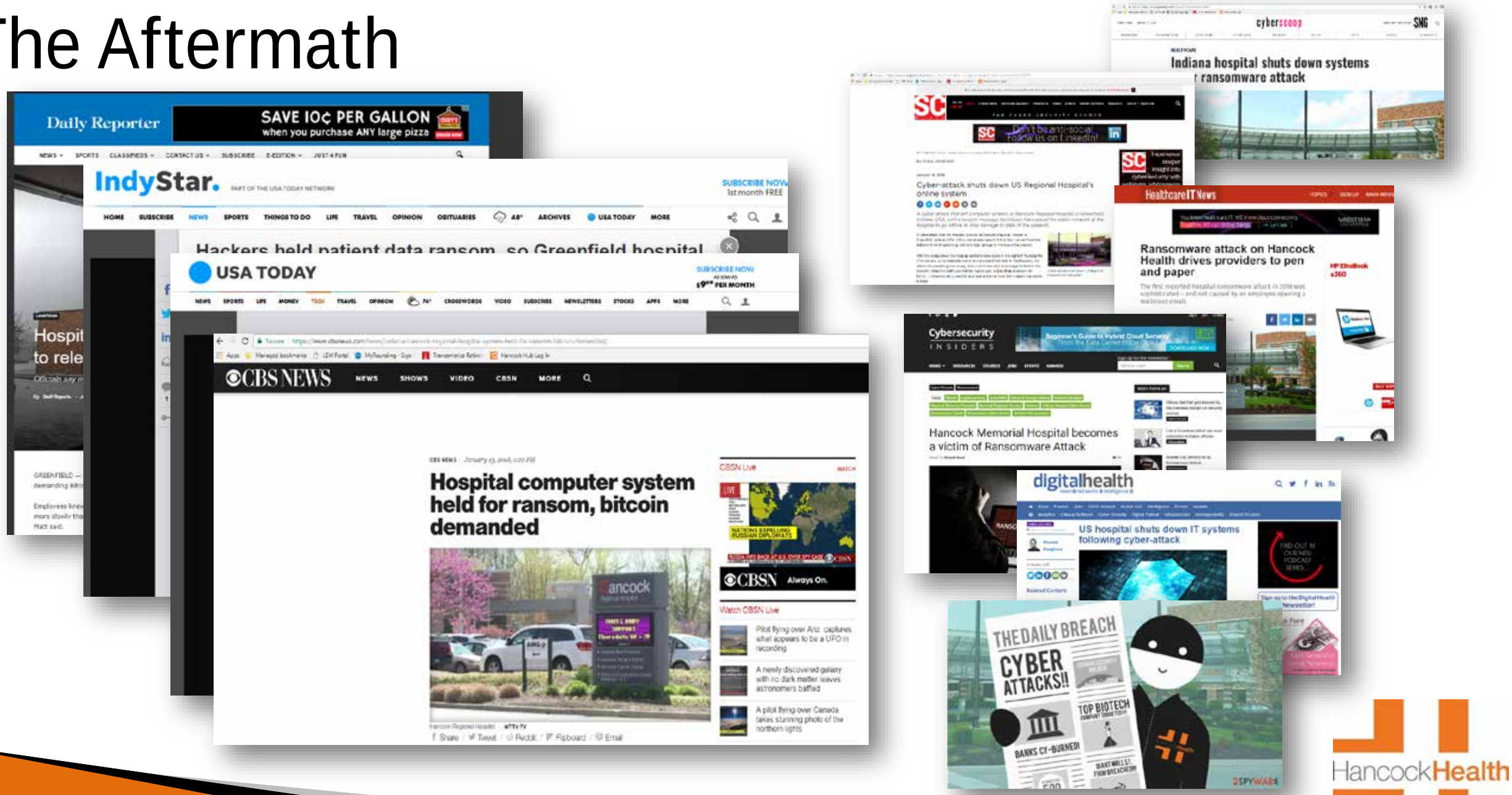
GREY'S ANATOMY



$20,000,000!!!

HancockHealth

The Aftermath



HancockHealth

I SURVIVED THE CYBERPOCALYPSE OF 2018
AND ALL I GOT WAS THIS SILLY T-SHIRT.

HANCOCKSTRONG

Strength *noun*

1 : the quality or state of being strong
2 : power to resist force | solidity, toughness
3 : power of resisting attack
4 : the ability to deal with difficult situations

The strength of Hancock Health is measured by our team of associates, doctors and volunteers. Our team is strengthened with the love and support of family and friends.

HANCOCK **STRONG**

Let's celebrate!

HancockHealth

HancockHealth

Craig Felty
317-468-4990
cfelty@hancockregional.org

HancockHealth™