HACKED :

The case of a hospital's data held HOSTAGE

HALL RENDER
KILLIAN HEATH & LYMAN

Presented by

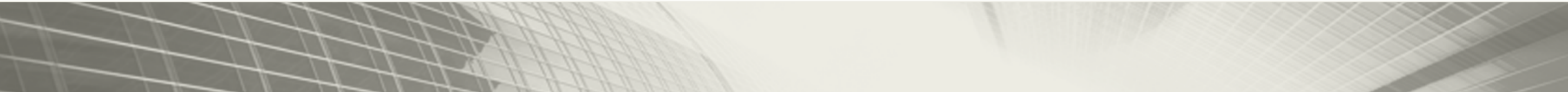
Mark J. Swearingen | (317) 977-1458 | mswearingen@hallrender.com

Overview

- Pre-Incident Conditions
- The Incident
- The Response
- The Legal Analysis
- Preparing for an Incident
- Preventing an Incident

Pre-Incident Conditions

- 20+ facility health system with over 1,200 staff that includes a 68-bed hospital, a multi-specialty physician practice, a women’s clinic, a cancer center, and a wellness center
- 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
- Inclement weather (ice storm)
- Heading into a long holiday weekend



The Incident

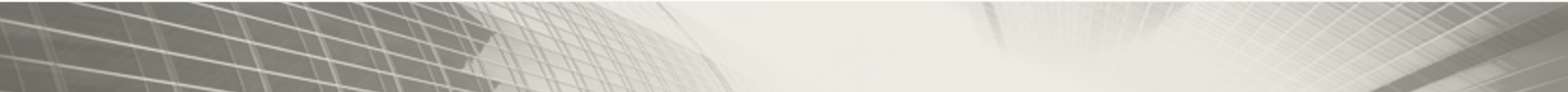
- Thursday at 9:30 PM: Messages began appearing on PC screens in the hospital indicating that the system was encrypted with SamSam ransomware and that decryption keys could be purchased four 4 Bitcoin.
  - One week deadline or data would be encrypted permanently
  - Message included step-by-step instructions for obtaining the decryption keys

The Response

- Activate Disaster Response Plan
- Initiate downtime procedures and stabilize patient care processes
- Contact key parties (legal counsel, IT forensics, FBI)
- Conduct IT forensic investigation
- To pay or not to pay?

The Response (cont.)

- Activate Disaster Response Plan
  - Immediate shut down of all network and desktop systems
    - Manual process involving approximately 1,200 units
    - Signs posted at all facilities noting all computers to remain off
  - Incident command center established by executive leadership
    - Communications by cell phone, text and non-system email

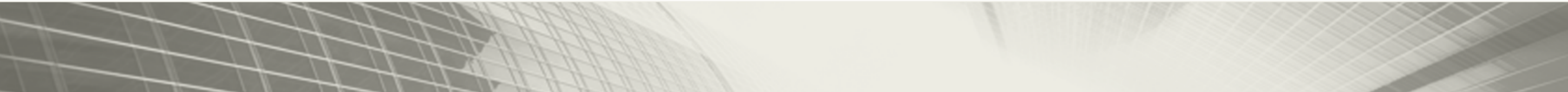


The Response (cont.)

- Downtime Procedures and Patient Care
  - 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.

The Response (cont.)

- Contact Key Parties
  - Friday at 4:00 AM: 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

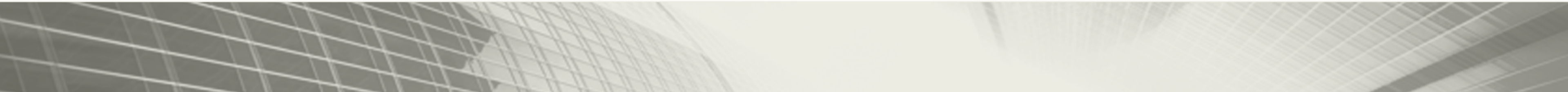


The Response (cont.)

- Conduct IT Forensic Investigation
  - Four stages:
    - Identification
    - Containment
    - Eradication
    - Remediation
  - Failure to follow this process could result in incomplete resolution and continuing incident.

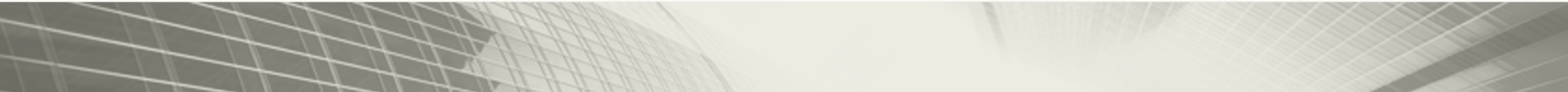
The Response (cont.)

- Conduct IT 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



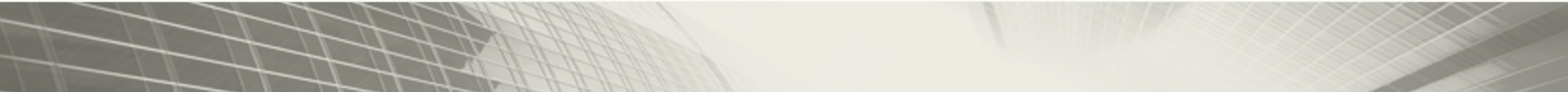
The Response (cont.)

- Ransom Demand: 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



The Response (cont.)

- Ransom Demand: To pay or not to pay?
  - 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



The Response (cont.)

- Ransom Demand: To pay or not to pay?
  - Decryption keys
    - Could be one key or many keys
    - Decryption process takes time also
- Restoring data and bringing systems back online is a slow and deliberate process

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?

Preparing for an Incident

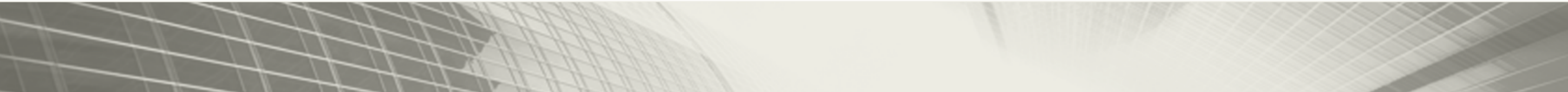
- Develop incident response plan
- Characteristics of an effective Incident Response Team:
  - Availability
    - Requires complete dedication to the task at hand
  - Selflessness
    - It’s not about you, it is about getting it right. No egos allowed.
  - Delegation
    - Trust your team. You can’t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

Preventing an Incident

- Conduct enterprise-wide risk analysis
- Develop and implement remediation plan.
- Regularly update and patch software and systems
- Implement two factor authentication
- Implement a vendor management program
- Conduct regular workforce training
- Obtain independent third-party penetration testing
- Implement managed security services to monitor IT activity, vulnerabilities and risks



Please visit the Hall Render Blog at http://blogs.hallrender.com for more information on topics related to health care law.

Mark J. Swearingen
317.977.1458
mswearingen@hallrender.com

This presentation is solely for educational purposes and the matters presented herein do not constitute legal advice with respect to your particular situation.

HEALTH LAW
IS OUR BUSINESS.
Learn more at **hallrender.com**.

HALL
RENDER
KILLIAN HEATH & LYMAN