Ransomware Incident Response - Panel

October 12, 2018

Jeremy Wulfekuhle

Medical Associates Clinic and Health Plan

- IT Director and Security Officer

Nathan Little

Gillware Digital Forensics

- Managing Partner

Edward Marchewka, MS, MBA, CISSP

CHICAGO Metrics™

- Founder
- Former Head of InfoSec for Chicago Public Schools
- "Version 1 is always better than Version 0."

4

Dominic Paluzzi

McDonald Hopkins

- Co-Chair, Data Privacy & Cybersecurity Practice

5

Forensics Perspective

- Preserving evidence
- Challenges specific to Ransomware - encrypted evidence
- Investigating to reasonable completeness
  - Avoid the "It probably was just an email attachment" philosophy

6

CISO Perspective

- Not if, but when…
- Preparation is key
  - Messaging
  - Notification requirements
  - Table top exercises

Attorney Perspective

- OCR Guidance on Ransomware
- "Whether or not the presence of ransomware would be a breach under the HIPAA rules is a fact-specific determination."
- "When ePHI is encrypted as the result of a ransomware attack, a breach has occurred because the ePHI encrypted by the ransomware was acquired (i.e., unauthorized individuals have taken possession or control of the information), and thus is a "disclosure" not permitted under the HIPAA Privacy Rule

Attorney Perspective

- In order to overcome the presumption of breach (and avoid notification), the covered entity or business associate must conclude, after conducting a risk assessment, that there is a low probability that the PHI has been compromised despite the ransomware attack
  - Utilizing 4 "standard" factors (extent of PHI; who is unauthorized party?; was PHI actually viewed?; extent of mitigation)
  - 2 "additional ransomware-specific" factors:
    1. Whether there is a high risk that the data will be unavailable
    2. Whether there is a high risk that data's integrity has been compromised.

Contact Info

- **Jeremy Wulfekuhle**
- jwulfeku@mahealthcare.com

- **Edward Marchewka**
- emarchewka@chicagometrics.com

- **Nathan Little**
- nlittle@gillware.com

- **Dominic Paluzzi**
- dpaluzzi@mcdonaldhopkins.com