UVM Medical Center Cyber Attack

April 2023

THE University of Vermont HEALTH NETWORK

What Happened?

- Not Ryuk – email phishing attack
- Encrypted 1300 servers – core infrastructure
- Malware on 5000 devices for persistence
- Epic not impacted directly
- No data breached

Immediate Response

Call to arms:

- Incident command
- Activated cyber security forensics retainer
- Contacted law enforcement

Red Button

- Shutdown all network systems
- Took down Epic
- Perimeter network lockdown
- BCA Mode

What Worked

- Close collaboration with law enforcement
- IT incident command
  - Operational Leaders
- Hospital incident command
  - Clinical and operational leaders
  - IT leaders attended (and vice-versa)
  - Prioritized system restore
  - Made clinical care and service decisions

Challenges

- Downtime procedures
- Communication
- Paper everywhere
- Remote workforce
- Daily clinical service decisions

Key Learnings

- Cyber security must be a top organizational priority
- Cyber security is an arms race!
- Ensure your downtime procedures and data anticipate a potential prolonged downtime
- Response to a cyber attack requires “all hands on deck” not just IT hands
- Review your cyber insurance plans now

UVMHN Security Standards and Frameworks

Regulatory

- HIPAA and the HIPSS security rule
- PCI DSS (payment card industry data security standard)

Internal

- Center for Internet Security (CIS) benchmarks and controls
- NIST Cybersecurity Framework (CSF)
- NIST Risk Management Framework (RMF) 800-37