24 Hours of a Medical Device Security Disaster

Adam Brand | PwC

cybersecuritysummit.org | #cybersummitmn
#whoami

• Adam Brand
  – Managing Director, Cybersecurity & Privacy
  – PwC
  – Focus on medical device security
Disclaimer

- Theoretical scenario
- Vulnerabilities based on previously reported vulnerability classes for medical devices
6:30am – Surgical ICU

ATTENTION!

All your medical device files were encrypted using a very advanced encryption system and a unique key.

To restore your files you have to pay only 50 BTC (bitcoin). This will unlock all devices in your hospital!

Don't delay and no patients will be inconvenienced.

Steps:
1. Create BitCoin wallet here: https://btcwalletsrus.com/wallet/new
2. Buy 50 BTC using a service from here: https://bitcoinlistingsofine.com/list
3. Send 50 BTC to this Bitcoin address: 2LA56f24nY8950
4. Open a decryptor link here:
6:35am – That Escalated Quickly

• Multiple departments
• 50% of nurses’ monitoring stations
• Most of imaging
• 80% of EEG carts
7:30am – Initial Reaction

• Divert new patients
• Canceling non-urgent procedures
• Additional staff called in
7:45am – Email to CMO

• “Getting ready to pay? Otherwise we can do more.”
8:00am – Recovery Update

• Missing installation software
• No recent configuration backups available
• Devices being re-encrypted once restored and reconnected
12:00pm – Recovery Update

- Subset of patients being moved
- Imaging systems recovery partially complete
- InfoSec and Networking collaboration

Missing Controls?
Integration w/Hospital
Emergency Ops Plan
2:00pm – Attacker Escalation Email

• “We see you are trying to fix without paying. We will show you what else we can do.”
2:05pm – Wave 2

• 25% of surgical systems
• Two fetal heart rate monitors in Neonatal Care
2:30pm – InfoSec Investigation

- Default credentials and missing patches being used
- Several attacker “hubs” throughout medical device network at key points
- Network and biomed team coordination

Missing Controls?
- ID & Access Management
- Secure Configuration
- Vulnerability Management
- Device Risk Assessments
6:30am, next day – Recovery Update

- 80% of devices recovered
- No re-infections
- Exhausted staff, concerned patients, newspaper stories
That was exhausting!

• Realistic?
• Close to home?
• What can we do?
What Could Have Mitigated This Attack?

- Response Plan
- Network Segmentation
- Recovery Plan
- Backups
- Malware Protection
- Configuration Management
- Threat Detection
- ID & Access Management
- Secure Configuration
- Vulnerability Management
- Integration w/Emergency Ops
- Device Risk Assessments

A holistic, multi-layered medical device security program.
How Are Others Going About This?

• Assessing their program and key risks
• Engaging the Board for risk decisions
• Building a holistic, multi-layered program
Key Questions/Next Steps

• Do you have a comprehensive medical device security program in place?
• Have hospital leaders been presented with the current state + need for investment?
• Has enough progress been made to mitigate attacks like this?