A DELPHI STUDY OF COUNTERMEASURES TO SECURITY THREATS IN NETWORKED MEDICAL DEVICES

Melinda Lyles

Agenda

- Problem Statement
- Purpose of the Research
- Research Questions
- Summary of Research Design
- Data Collection Process
- Data Analysis Techniques
- Summary of Findings
- Summary of Conclusions
- Summary of Implications
- Recommendation for Future Research

Problem Statement

- Lack of effective countermeasures for cyber threats to networked medical devices:
  - attack on a medical device is likely to occur;
  - risks between networks and medical devices;
  - security risks leading to unauthorized personnel;
  - breach with sensitive data pertaining to PHI.

Purpose of the Research

- Create a model for developing effective countermeasures for cyber threats
  - Networked medical devices;
  - Healthcare industry;
  - United States.

Research Questions

What are the relevant experiences in employing a schema to analyze security risks in networked medical devices?

Summary of Research Design

- **Method:** Qualitative Research
- **Design:** Delphi Study
- **Sample Size:** 15 IT experts in healthcare experience with medical devices
- **Rationale:** developed a model for effective countermeasures based on experiences and perceptions of IT experts in the phenomenon with networked medical devices
- **Selection Criteria:** IT experts working in the health field

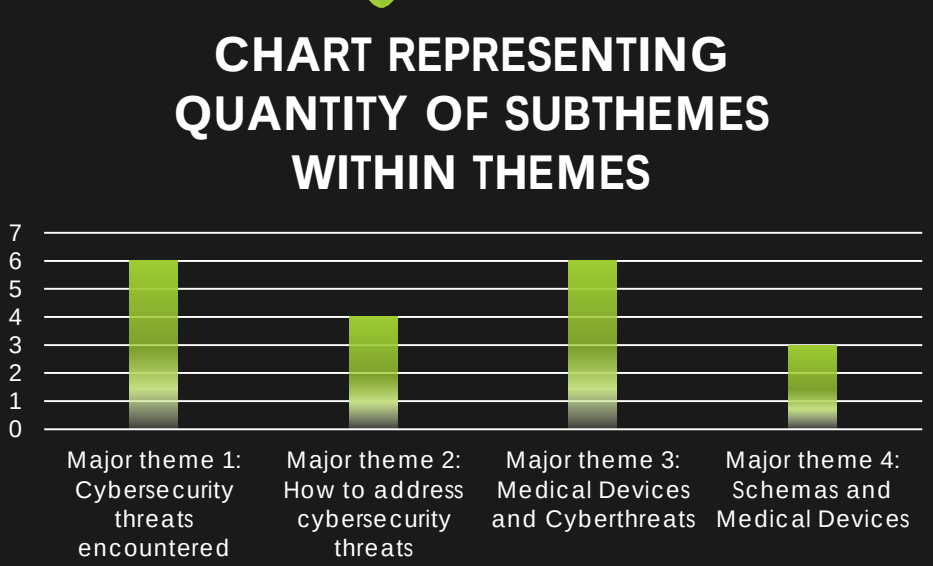
Data Collection Process

	Identify IT Experts	(a) Recruitment (b) Purposive Sampling (c) IT expert criteria
	Thematic Development	(a) Open-ended interviews (b) Three rounds of interviews (c) Categorized responses
	Thematic Consensus	(a) Theme consensus developed (b) Reaching data saturation
	Results Analysis	(a) Theme analysis (b) Comparison analysis (c) Reviewed business technical problem with results

Data Analysis Techniques

- First round: thematic analysis
- Second round: frequency graph
- Third round: summary of confirmed results

Summary of Findings



- Major theme 1: Cybersecurity threats encountered
  - Subtheme 1a: Configuration Management
  - Subtheme 1b: Wireless and Bluetooth Connection
  - Subtheme 1c: Internet of Things
  - Subtheme 1d: Data Breaches
  - Subtheme 1e: Insider Threat
  - Subtheme 1f: Asset Management
- Major theme 2: How to address cybersecurity threats
  - Subtheme 2a: Controls assessment
  - Subtheme 2b: Automated technology
  - Subtheme 2c: Policy changes
  - Subtheme 2d: Security awareness and training
- Major theme 3: Medical Devices and Cyberthreats
  - Subtheme 3a: Security measures
  - Subtheme 3b: Cybersecurity Failures Experienced
  - Subtheme 3c: Addressing Cybersecurity Failures
  - Subtheme 3d: Reasons for Failure
  - Subtheme 3e: Prevention of Failures
  - Subtheme 3f: Analytical Tools for Security Risk
- Major theme 4: Schemas and Medical Devices
  - Subtheme 4a: Successful Schemas
  - Subtheme 4b: Differences between Schemas
  - Subtheme 4c: Failures with schemas

Summary of Conclusions

- Semi-structured interviews
- Risks and networked medical devices were not monolithic,
- Fulfillment of the Study was completed
- Identification
  - Protect
    - Controls Assessment
    - Automated technology
    - Policy changes
    - Security Awareness and Training
  - Apply
    - Real-time
    - Manual Implementation
    - Mitigation Risk
  - Address
    - Lockdown
    - Report
    - Run automated

Summary of Implications

- IT Experts agreed that manufacturers are crucial within the process of implementing security when developing and throughout lifecycle of the device.
- Clinicians or patients remain uneducated about the methods for evaluating security risks with networked medical devices;
- Impacts for IT Support and organizations supporting networked medical devices enhance improve upon cybersecurity and device awareness;
- Scholars may leverage the model developed, employing increasing efficiency identifying areas of risk

Recommendation for Future Research

- Explore and examine
  - how patients use medical devices
  - how such behaviors impact issues of security
  - public perceptions of cyber healthcare risks associated with the use of medical devices and if such perceptions alter the use of devices and/or individual health outcomes
  - Hospitals from which these devices come
    - How do hospitals create IT policy based on cybersecurity risk?
    - In what ways do the organizational elements of the hospital dictate how they manage cybersecurity risks?

Continue Recommendation for Future Research

- Using the model developed
  - gauge how such a model is successful in helping prevent cybersecurity attacks on medical devices
- Using a Case Study
- how this model aids specific hospitals, or specific types of medical devices, from cyberattacks
- Regulations
  - State to state
  - State to Federal
  - Variance with cybersecurity comparing different medical devices