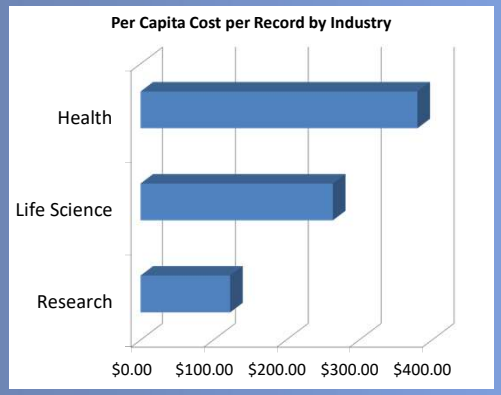
Legal Implications of Nanotechnology through a Cybersecurity Lens: A Healthcare Case Study

Derek J. Sedlack, PhD – Craig Vrabec, JD

Introduction:
Increasing reports of hacked medical devices put nanotechnology at risk with larger, more traditional infrastructure. Even while our programming languages evolve and information security has become part of the spotlight, we continue to experience data breaches. The inherent design of Nanotechnology presents the two additional risk constructs of litigation and cybercrime.

Research Problem:
How to shift the design focus of medical devices (including nanotechnology) and mitigation factors to improve an organizational legal and cybersecurity posture.



Research Questions:

Three research questions will guide the research:

1) Can data loss be linked to frame incongruity?

2) How do healthcare technology designers view potential client legal risks?

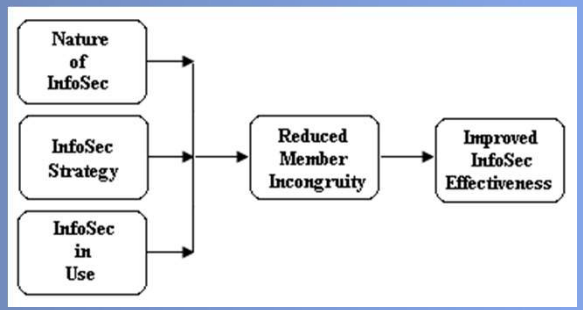
3) Does the organization consider cyber- and legal-risks as competing, supporting, or interrelated?

Methodology

Theoretical Basis:

The theoretical basis utilized in this research is a business view case study approach based on the continued illicit manipulation of technology and increasing litigation factor of organizational data loss. The case study will focus on organizational effectiveness, specifically information security as relating to data collecting devices through the Information System Security Frame Alignment Model (ISSFAM). If organizational group perceptions are sufficiently rigid, the gaps created increase overall organizational risks and legal exposure.

Proposed Theoretical Model:



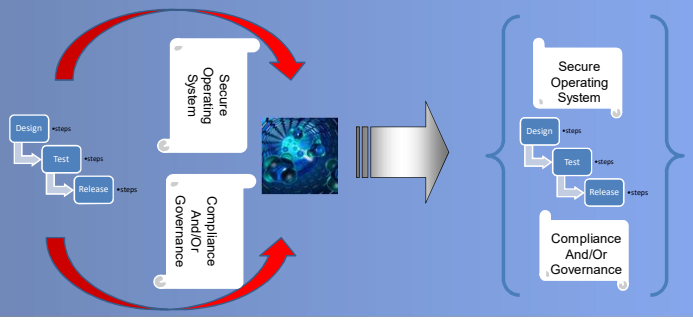
Research Design:

Qualitative | Case Study: Business Approach

- **Identify Decision Makers**
- **Understand Technology Risks (through Betts)**
- **Frame Legal Foundations**
- **Integrate Tech Risks with Legal Exposure**

Research Approach:

- **Identify nanotechnology manufacturers and integrated software engineers within targeted healthcare verticals.**
- **Select a project with a practitioner that is simple and iterative in nature.**
- **Coordinate with practitioner to iteratively modify or restrict designs to reduce cyber and legal exposure.**
- **Determine model effectiveness through practitioner feedback and collected data.**



Expected Outcome:

Legal exposure will decrease and the information security posture (defensibility) will increase as a result of realigned perceptions of associated risks relating to technology designs commonly associated with data loss and exposure, leading to better alignment with organizational objectives. This model could be applied departmentally or inter-organizationally for further alignment improvements.