What Would YOU Do?

You are on the Board of Directors (and the Chair of the BoD subcommittee, Cybersecurity Oversight) of a Community Hospital and There is a Cybersecurity Crisis.

John Mumford – President & Founder
Fellsway Group, LLC

Situation Overview

Community Health Hospital, a key healthcare provider in a suburban community, faced a cyber-attack where hackers encrypted vital patient records and demanded a ransom. The CEO favored a discreet approach – paying the ransom and upgrading systems quietly – to avoid public panic and ensure continuity of care. Conversely, the Board Chair advocated for openness and public engagement, concerned that secrecy might damage the hospital's credibility and trust within the community.

You are the Chair of the Cybersecurity Oversight Committee. The Chair calls you on the phone and asks your view of the next steps from a Board perspective.

Assumptions

Business Revenue: $225M

Ransom Amount: $5M

Detailed Analysis

1. **Strategic Decision Factors**:

    - **Immediate Response**: The CEO's strategy to quickly restore services by paying the ransom and secretly upgrading systems aimed to minimize service disruption and prevent public fear. However, this short-term solution risks future security by potentially encouraging further attacks.

    - **Long-Term Impact**: The Chair's approach focused on ethical transparency, foreseeing that integrity and openness would foster long-term community trust and resilience.

2. **Ethical Implications**:

    - **Moral Responsibility**: The hospital holds a moral duty to protect patient information and ensure the community's well-being. Quietly paying the ransom

could be seen as capitulating to criminal demands without addressing the root cause.

- **Stakeholder Trust**: Maintaining stakeholder trust is crucial for a community hospital. Secrecy could erode this trust, whereas transparency, even about failures, could enhance credibility.

3. **Operational and Financial Considerations**:

- **Cost Analysis**: Weighing the cost of ransom payment against the investment in robust cybersecurity measures. Immediate payment might seem less expensive but doesn't factor in the long-term costs of potential repeated attacks.

- **Resource Allocation**: Evaluating whether existing resources could be redirected for system upgrades or if additional funding would be necessary, potentially through public support or increased healthcare premiums.

4. **Legal and Regulatory Compliance**:

- **Compliance with Laws**: Analyzing legal obligations under health information privacy laws (e.g., HIPAA in the U.S.) which may require disclosure of breaches affecting patient information.

- **Reporting Obligations**: Understanding the implications of not reporting the ransomware attack, which could involve fines and legal repercussions, impacting financial stability and public image.

Questions for Consideration:

- **Ethical and Strategic Considerations**
  - **Transparency vs. Confidentiality**:

    - How do we balance the need for public transparency with the potential for causing unnecessary panic among our patients and community?

    - What are the potential long-term implications of keeping the ransom payment and system upgrades confidential?

  - **Decision-Making in Crisis:**

    - What criteria should guide our decision on whether to pay the ransom or not? Should the potential recurrence of attacks influence this decision?

    - What are the core principles that should guide our response during a cybersecurity crisis? How do we ensure these principles are consistently applied?

    - What role should the Board of Directors play in crisis decision-making to ensure both swift action and adherence to our ethical standards?

    - What strategies can we develop to mitigate the risk of recurrence if we choose to pay the ransom? How can we communicate these strategies to our stakeholders to maintain their trust and confidence?

- **Financial and Operational Impact**
  - **Resource Allocation:**

    - Considering the immediate need for upgrades, how should we prioritize spending on cybersecurity versus other critical hospital needs?

    - What financial strategies can we implement to enhance our cybersecurity infrastructure without compromising patient care and other essential services?

  - **Fundraising and Community Support:**

    - How can we effectively communicate the need for financial support to the community and local government? What are the key messages to convey the importance of their contributions?

  - **Cyber Insurance Coverage:**

    - What specific aspects of cyber incidents does our current cyber insurance policy cover? Does it include ransom payments?

    - If our cyber insurance does not cover the ransom, what financial strategies should we consider to manage the potential costs effectively?

- **Funding Ransom Payments:**
  - If we decide to pay the ransom, from which budgetary allocations or financial reserves should the payment be sourced?
  - What financial safeguards can we implement to ensure that paying a ransom does not severely impact our operational budgets or financial stability?

- **Legal and Compliance**
  - **Regulatory Compliance:**
    - How do our current policies align with legal requirements for reporting cyber incidents? Are there any gaps that need to be addressed immediately?
    - What are the potential legal consequences of not reporting the ransomware attack or of reporting it late?

  - **Legal Restrictions:**
    - How can we verify whether the party demanding the ransom is not on any sanctioned lists? What are the legal implications if they are?
    - What protocols should we establish to quickly assess the legality of making a payment under such circumstances?

  - **Data Privacy and Security:**
    - What steps can we take to strengthen our compliance with data protection laws and enhance patient data security?
    - How can we better prepare and equip our staff to handle data responsibly and recognize potential cybersecurity threats?

- **Organizational Structure and Long-term Strategy**
  - **Role of the Cybersecurity Oversight Committee:**
    - What specific responsibilities should the Cybersecurity Oversight Committee have compared to the Audit Committee?
    - How often should this committee meet, and what metrics or outcomes should they report to the Board?

  - **Future Incident Prevention:**
    - What are the key components of an effective incident response plan for future cybersecurity threats?
    - How can we integrate lessons learned from this incident into our ongoing training and development programs for all employees?

Community Engagement and Public Relations

- **Managing Public Perception:**

- How should we manage the narrative around the cyber-attack to rebuild and maintain public trust?

- What are effective ways to demonstrate our commitment to transparency and security in our communications with the public?

- How might paying a ransom, especially to a potentially sanctioned entity, affect our hospital's reputation both locally and in the broader healthcare community?

- **Community Involvement:**

  - In what ways can we involve the community in our cybersecurity initiatives to foster a sense of shared responsibility and trust?

  - How can community feedback be incorporated into our cybersecurity planning and response strategies?