Cyber Threats, Risk Management Efforts and the Importance of Communication

Fernando Martinez PhD CISSP CISM CISA CGEIT
Chief Strategy Officer

Technology and technology architecture

represent the greatest impact risk to the organization and the mission they serve.

- Nearly everything in an organization depends on technology, and it is increasing. Even if everything else works perfectly, the core mission can be compromised by a technology failure.

- The rate of technology development is disproportionately faster than an organization's ability to adapt and adopt. Think Generative AI, and the impact to providers and payors, and BOTS. Claims, appeals and FTE’s.

Addressing Risk

Does not need to mean additional spend

- Medical device security vs. effective exploit vectors
- The need to balance budget/spend and risk management effectiveness and completeness
- Understanding risk appetite from a cyber security perspective (ERM)

Relationship and communications channels

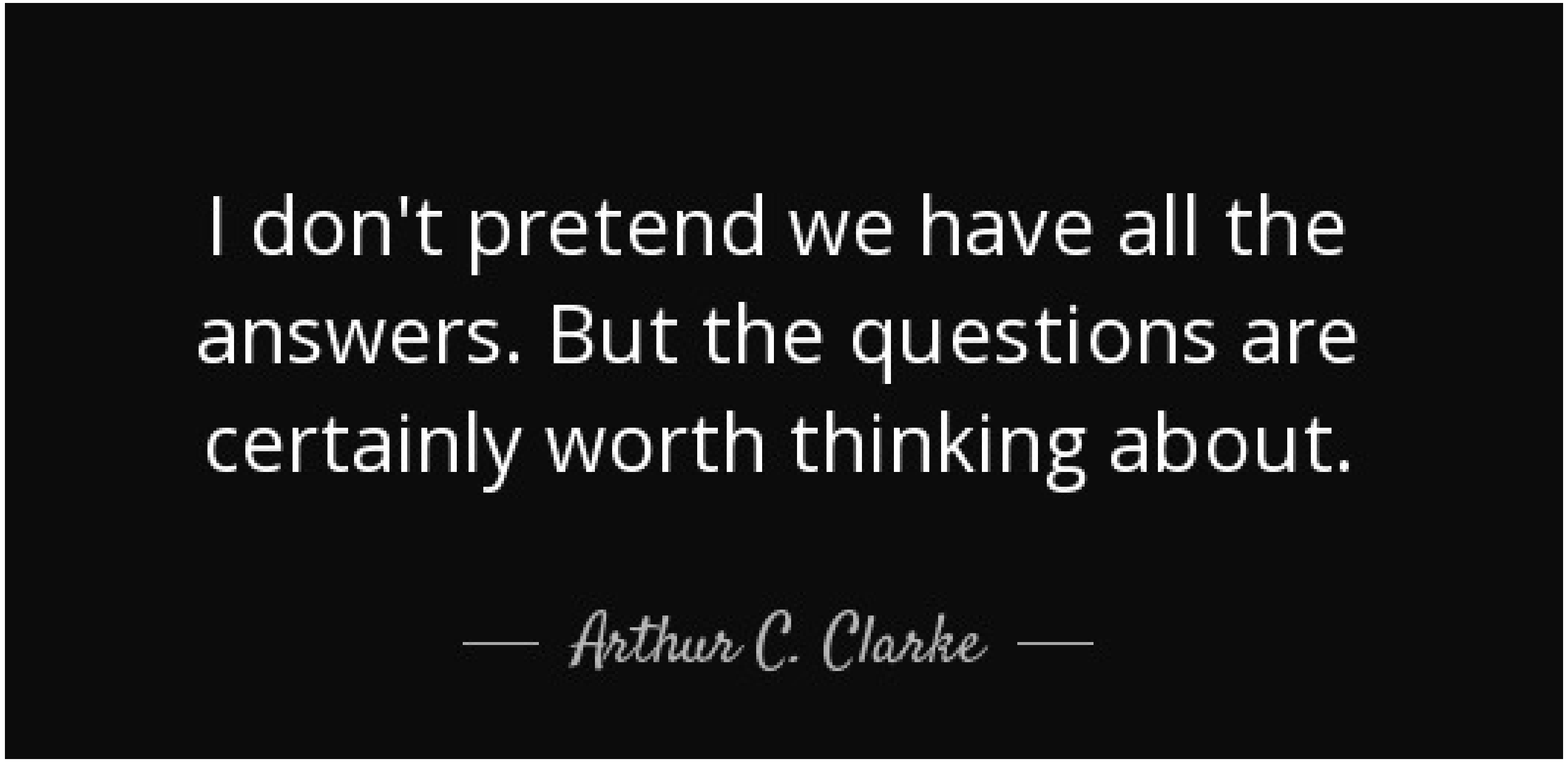
between IT executives and Sr. leaders are critical

- Trust/individual judgement vs. ROI/TCO/Cost benefit
- Inherent challenges of nomenclature/terminology.
- Difficulty in assessing competence of individuals leading architecture, design, management,
- The accelerating evolution of technology
- The race against evolving threat actor tactics

Few organizations rehearse cyber incident

detection, reaction, response, and recovery. Even fewer do it on a recurring basis

- The core of emergency preparedness is rehearsing a potential incident. Simulating disasters forces staff to respond under unplanned, variable circumstances.
  - this has been done for years with mass casualty events.
- Best area of opportunity for risk management reduction. And ultimately, the risk we are reducing is the risk of harm to patient outcomes.



I don't pretend we have all the answers. But the questions are certainly worth thinking about.

— Arthur C. Clarke —

Questions worth thinking about

- How and who can declare a breach or incident
- Who in leadership is contacted, what about the board, Cyber Insurance policy expectations for notification, FBI, or other law enforcement
- What is the incident response plan, who has it, how do you reference it?

Questions worth thinking about

- Who are the incident response team members, not just from IT, but from operations? And who are their backups?

- And what authority do they have? Who is authorized to and knows how and where to disconnect from the internet? What is the collateral impact to other internet dependent processes or resources, or partners.

- Same questions would apply to a third-party vendor or solution provider. Do you know their plan, their IRT, the names, roles, contact information of the staff?

Questions worth thinking about

- Is there an impact to clinical operations, surgical schedule, medical staff

- If you must revert to manual, where are the forms you will need and what downtime computer or data source can you rely on for patient care

- Is there an impact to other area hospitals, emergency response professionals, medical providers

Questions worth thinking about

- If there is a ransom to consider, who has a digital wallet, where do you get bitcoin, should you negotiate, who will negotiate, does your cyber liability policy have requirements?

- John Riggi, formerly with the FBI now with the AHA works very closely with the FBI and CISA.

Board accountability of hospital leadership

where cyber risk and organizational resilience is concerned is very inconsistent and infrequent

- How will you know if the attackers are still present?
- Has the data breach been stopped/contained?
- What is the scope of the breach? What was stolen
- What type of data was encrypted or stolen (or both).
- Is this a violation of HIPAA or other data privacy regulations?
- Who has been affected?

SO MUCH TO THINK ABOUT

- Consumerism and the impact on what technology wants to automate in the world of hospital IT
- The difference in the speed of evolution and development of technology versus a hospitals ability to evaluate the technology, adopt the technology, train staff and operationalize
- Potential threat that may come from regulatory changes that aim to compel different behavior in hospitals and how they view resilience. (Cyber Security Performance Goals)

https://hphcyber.hhs.gov/performance-goals.html

- Change Healthcare and third (or fourth) party risk

Thank You

Fernando Martinez PhD
Texas Hospital Association
1108 Lavaca Street, Suite 700
Austin TX 78701

fmartinez@tha.org

Join the conversation by connecting with me:
http://Linkedin.com/in/fmartinezphd