Cyber Risk *is* *Enterprise Risk*

12 Areas for Leadership Consideration

Presented by John Riggi, Senior Advisor

Cybersecurity and Risk

February 19, 2020

American Hospital Association™
Advancing Health in America

AHA CENTER FOR HEALTH INNOVATION

AGENDA

- Audience Questions
- 12 Areas for Leadership Consideration
- Discussion and Questions

Baseline Cyber Risk as Enterprise Risk Questions

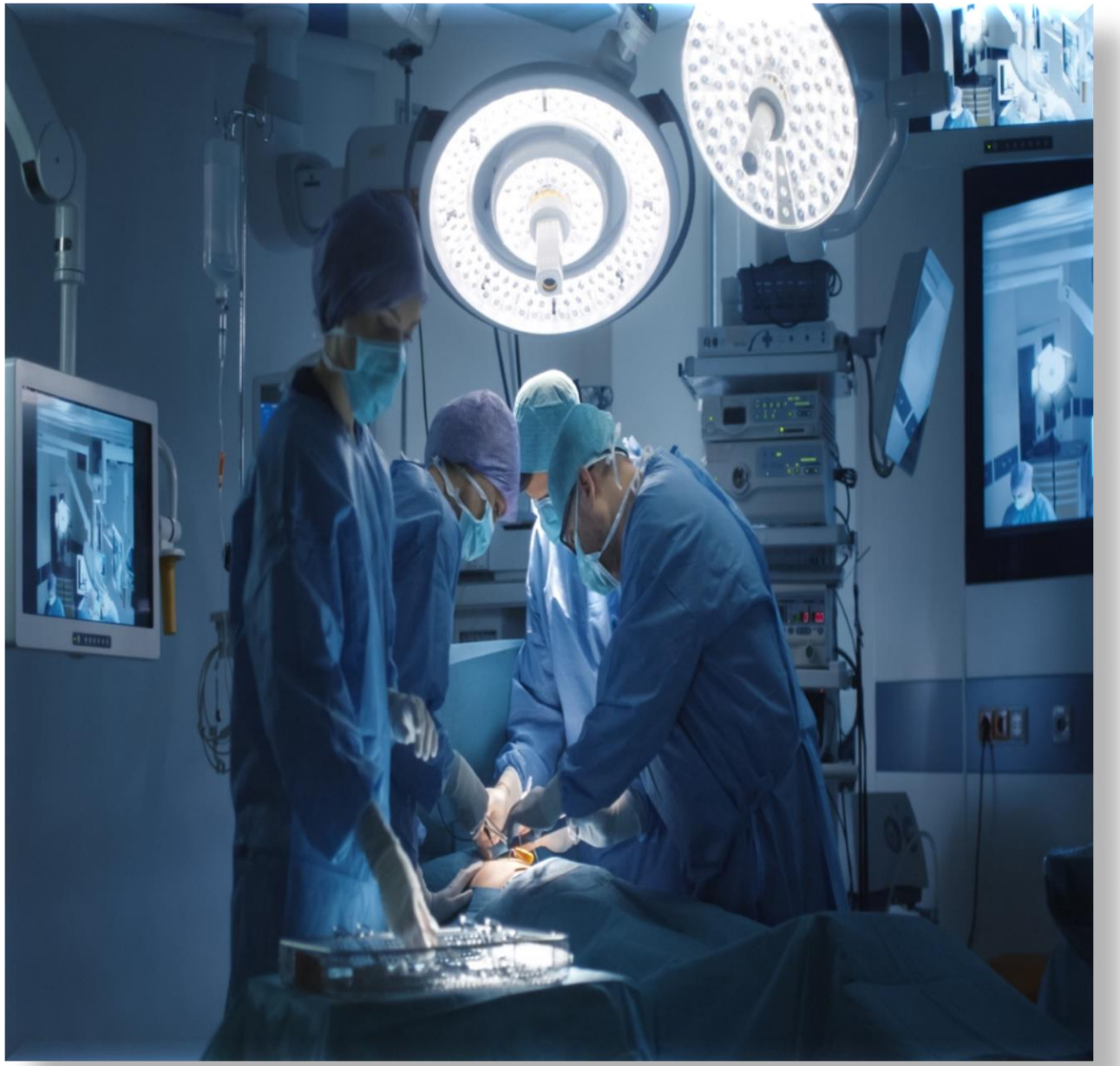
- In your organization, is cyber risk ranked as enterprise risk?
  - If so, is it ranked within the top **5**?
    - Top **3**?
      - Number **1** enterprise risk issue?

  - *Why is cyber risk an enterprise risk issue for your organization?*

- How often is cybersecurity briefed to the board?
  - What board committee has oversight and how are they engaged?

- Is the cybersecurity budget measured as a % of the IT budget or the enterprise budget?

- How does your cybersecurity budget compare to the healthcare industry average?



1. Patient Safety, Medical Devices and Mission Critical Systems

- What are our most ***mission-critical, life support and care delivery*** systems, devices and networks? How vulnerable are they to cyberattacks?
- What percentage are vulnerable and what is the ***plan and timetable to mitigate the most critical risks***?
- *Do we have a process to maintain an* ***accurate, dynamic inventory*** *of our network capable medical devices*?
- How are medical devices protected and **segmented** from other networks?
- Is there ***effective formal coordination and processes*** between the information security and the biomed engineering teams ***for acquisition and patching of medical technology?***
- ***Network mapping?***

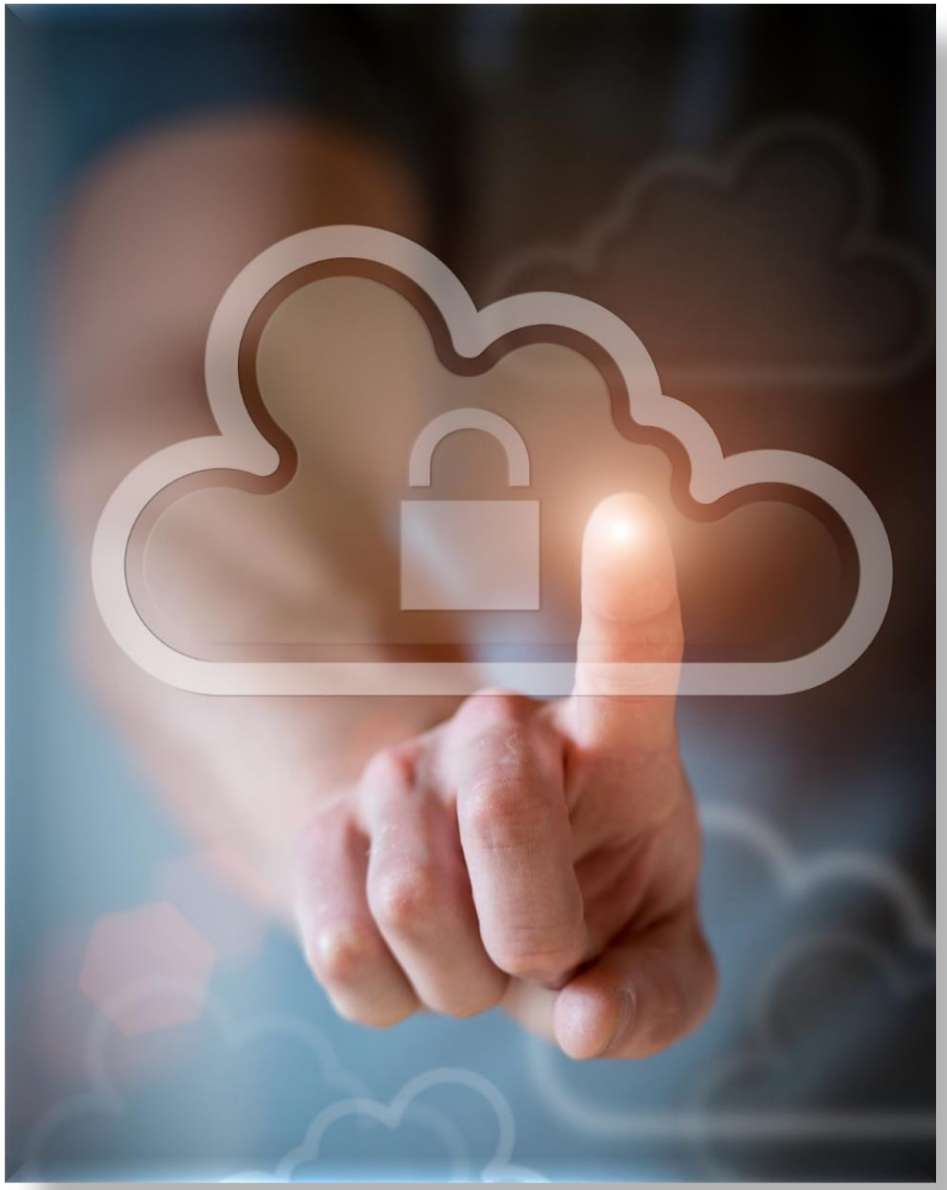
2. Strategic Cyber Risk Profile

- What is our strategic cyber risk profile, from the adversaries' perspective, based on the identification of our most valuable data sets, access to patients and network connections?
- How are we impacted by strategic risk related to geopolitical events, emerging technology and emerging cyber threats.
- What are our external sources of threat intelligence to inform our assessment?
- Who is coming after us (e.g., nation states, criminal organizations, insiders or a combination)? How and why?
- Have we mapped all our internal and external network connections? Have we mapped our data and baselined network activity?
- Clinical integration risk and regulatory driven risk?

3. Tactical and Technical Cyber Risk Profile

What is our current state technical and tactical cyber risk profile based on our latest risk assessments:

- Our policies, procedures and controls
- Vulnerability and penetration testing of our technical environment
- Cybersecurity maturity level of the organization based upon a recognized framework or chosen measures?
- How do we compare to other similarly situated organizations?



4. Risk Prioritization and Impact

Do we prioritize all strategic threats, cybersecurity policies, procedures, controls and technical risks by ***impact*** to:

REPUTATION

1. ***Care delivery and PATIENT SAFETY - first and always***
2. Mission critical operations
3. Confidence of patients, staff, community and investors
4. Protection and privacy of data - including health records, personally identifiable information, financial and payment data and ***intellectual property****
5. Revenue
6. Legal and regulatory exposure
7. Mergers and acquisitions

Strategic Cyber Risk Identification, Assessment and Prioritization

(THREAT + VULNERABILITY + IMPACT)

x (PROBABILITY + VELOCITY)

=

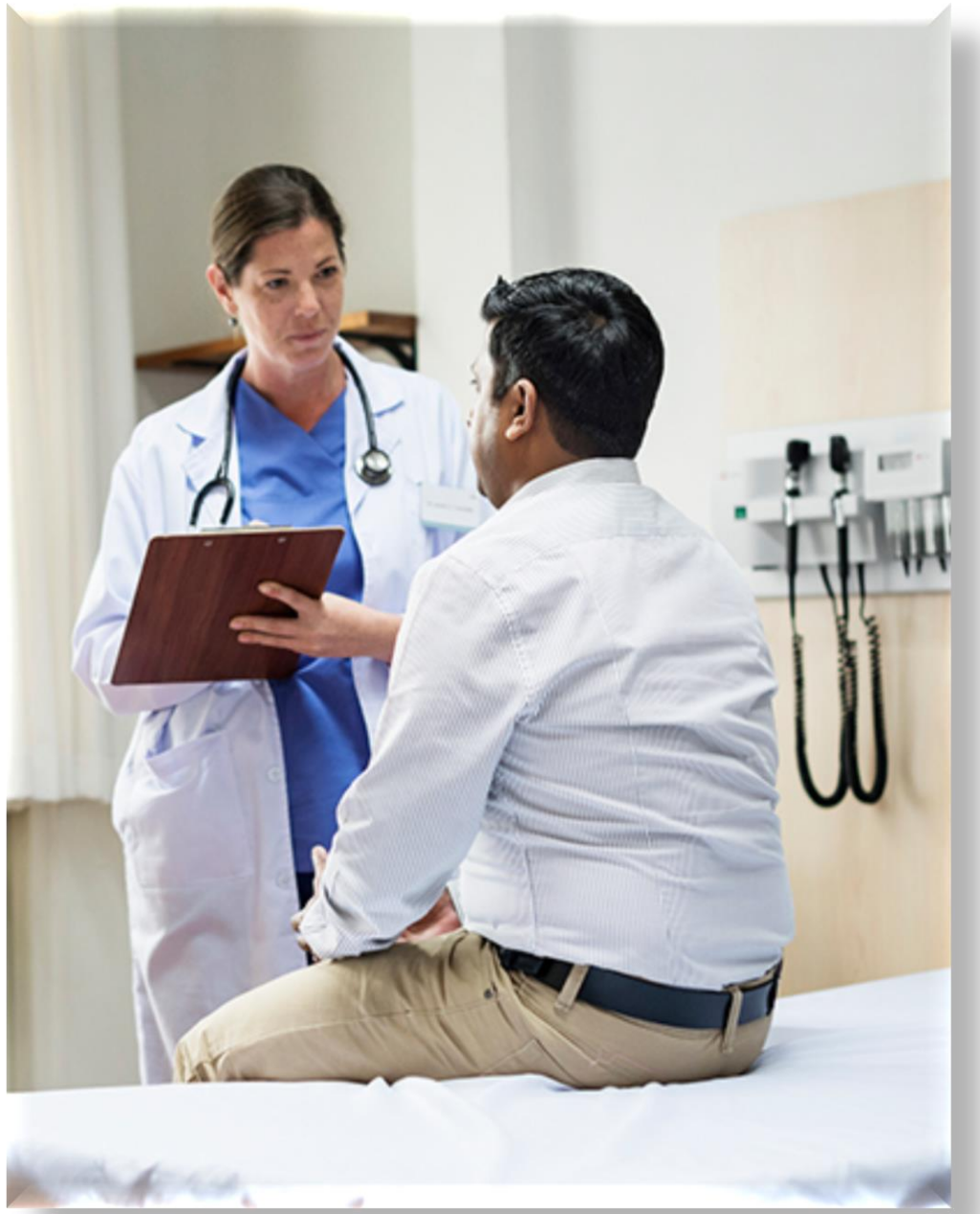
RISK PRIORITIZATION

5. Vendor Risk Management Program

- Does the organization have a vendor risk management program?
- How involved is cybersecurity in the process?
- Does the vendor agreement include cybersecurity and cyber insurance requirements?
- Have we conducted a recent in-depth technical, legal, policy and procedural review of our vendor risk-management program.
- Have we identified and **risk classified** vendors and their subcontractors based upon:
- **Aggregation** of data
- **Access** to sensitive data, networks, systems and locations
- **Criticality** to continuity of operations
- **Foreign** operations and foreign subcontractors
- How do we balance the financial opportunities, greater supply-chain flexibility with potentially higher cyber risks?

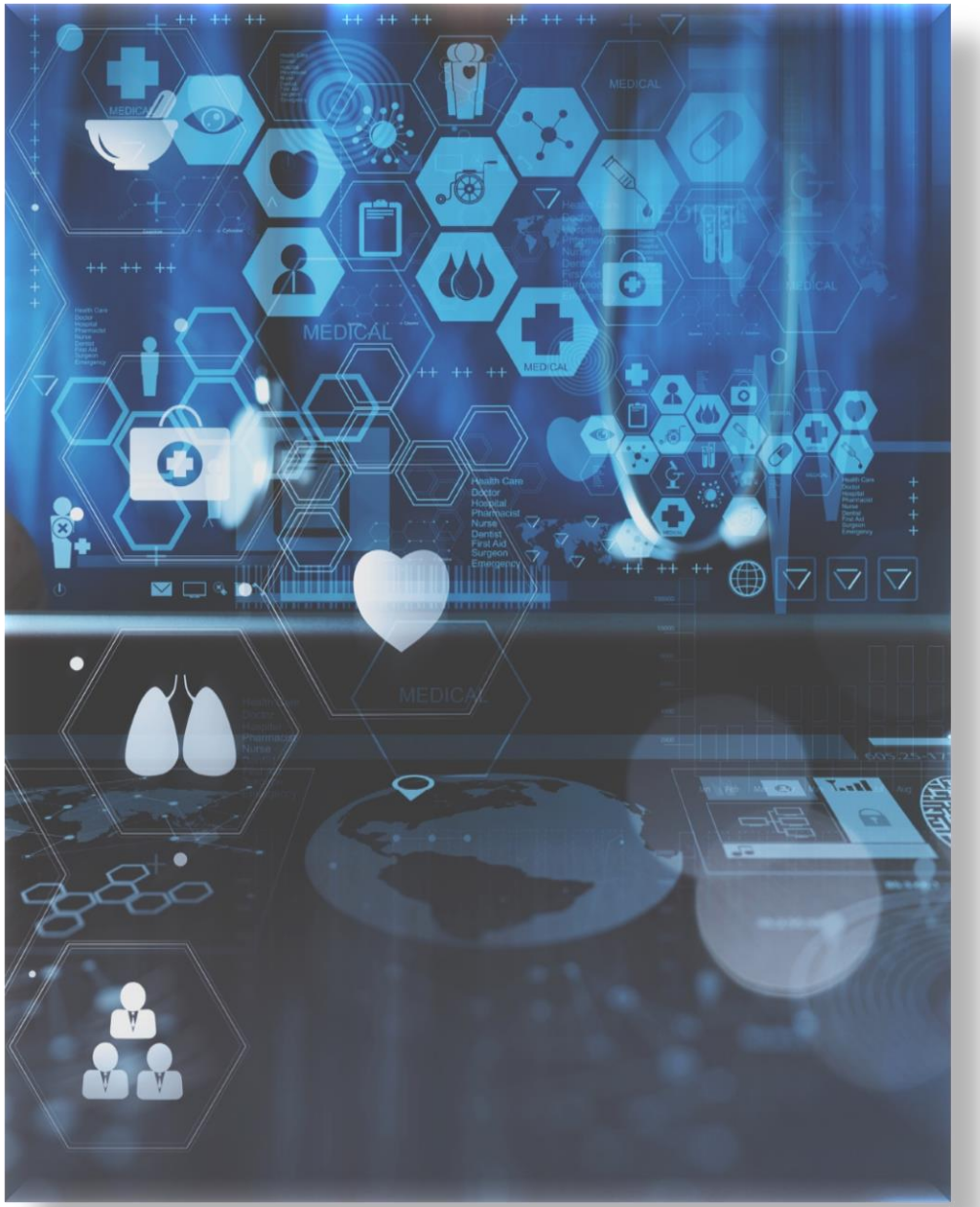
6. Capabilities, Resources and Governance

- Based on our strategic and tactical risk profile, are we certain we have sufficient and capable human and technical resources along with a **sufficient budget** devoted to our cyber security program?
- Do we have a Chief Information Security Officer (CISO) or someone devoted full time to security?
- Does the reporting structure of the CISO/Cyber lead provide sufficient status, authority and independence to be fully effective in protecting patients and the organization? Conflict of interest?
- What board committee oversees cybersecurity, how are they engaged and how often are they briefed?



7. Cybersecurity Culture

- What is the cybersecurity culture of our organization?
- Compliance based or risk based?
- It's the end users, ***the people***, who are ***being targeted*** and represent ***the best defense*** against cyber threats ***or the greatest vulnerability.***
- Is leadership engaged and actively support a culture of cybersecurity? How?
- What is the phishing test click rate?
- Is there a documented cybersecurity/HR sanctions and rewards program for staff?
- ***Leverage your existing culture of care!***
- ***Cyber hygiene is as important medical hygiene!***



8. Risk Mitigation Strategy and ERM

Based on our current cyber:

a. Strategic and technical **risk profile**

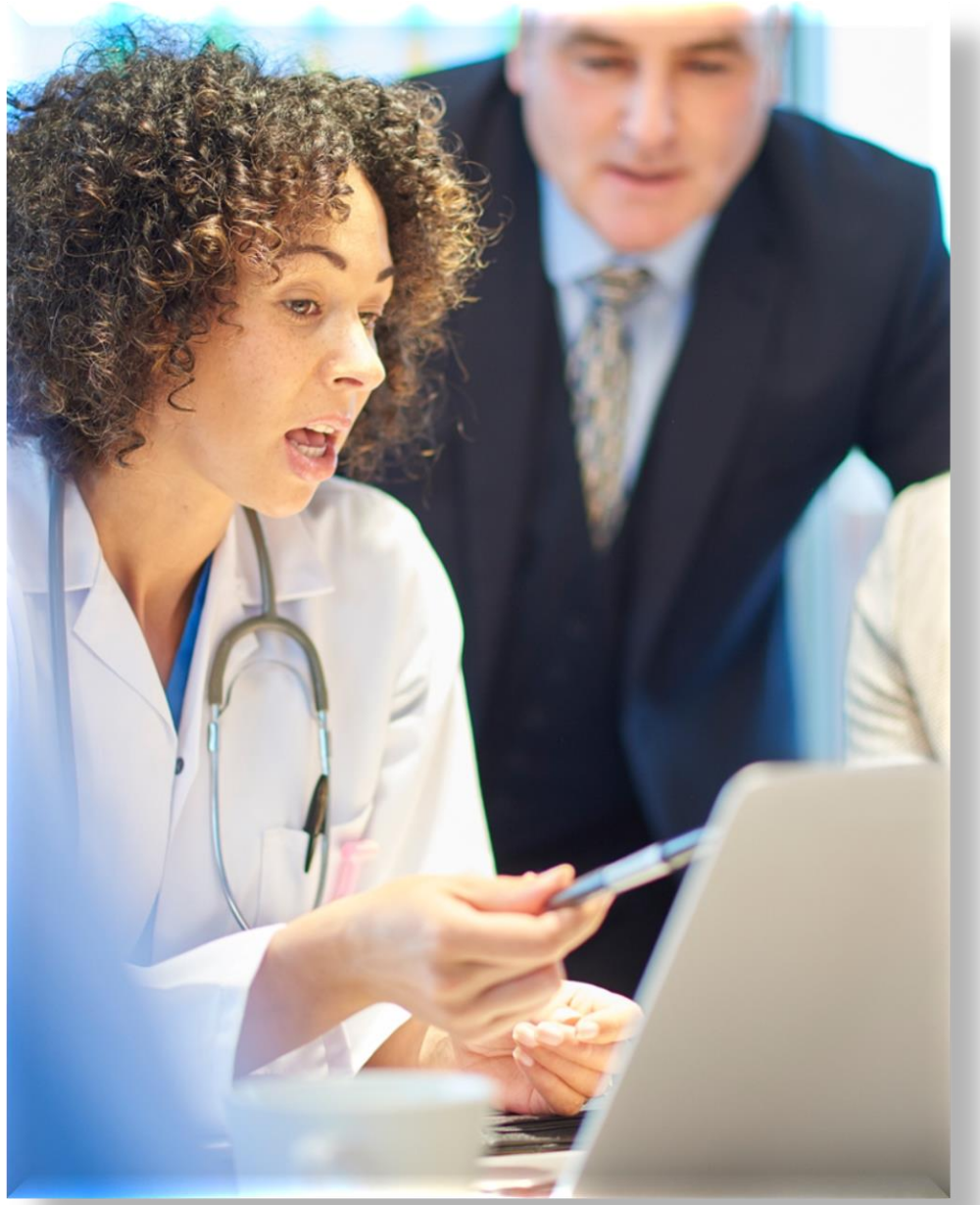
b. **Culture** of cybersecurity and our

c. **Target** cyber risk profile and cyber maturity level

d. **Risk tolerance** level

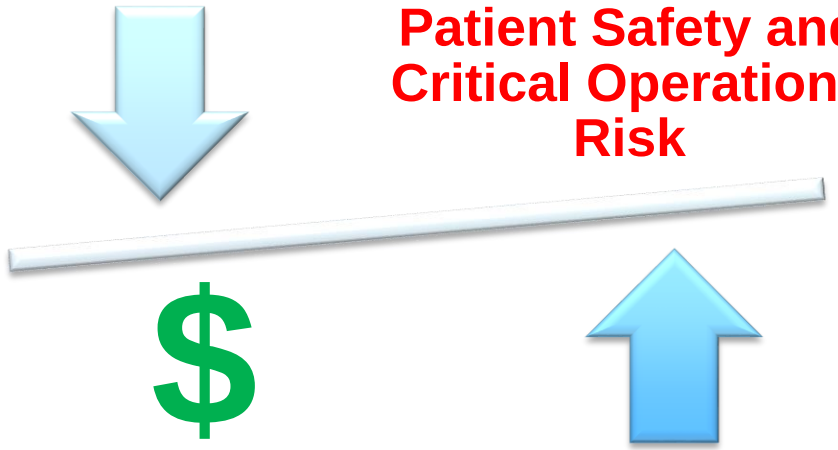
What is our cyber risk mitigation strategy?

- Is it integrated into an overall multidisciplinary, enterprise risk-management program and governance structure?
- What enterprise risk priority is cyber risk?
- How is the cybersecurity budget measured? Against IT or enterprise budget? Industry?
- Do we follow a particular cybersecurity framework? Why or why not?
- What measures or metrics are used to track and report progress in cybersecurity?



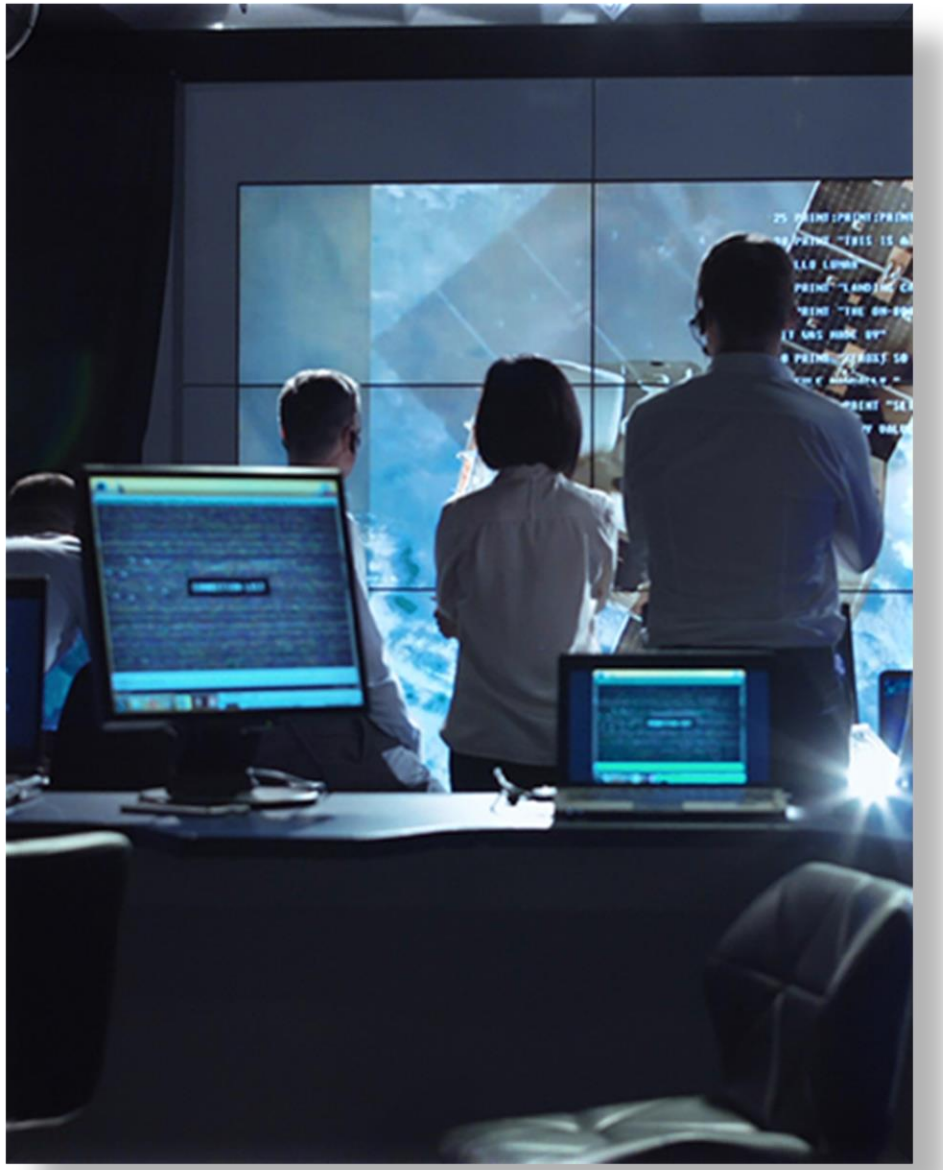
9. Risk Mitigation Implementation Plan

- What is our cyber risk mitigation strategy implementation road map?
- Are there specific program objectives, milestones and timeline?
- Is there a cost/benefit analysis review for each objective in terms of risk reduction impact to **patient safety / critical operations?**



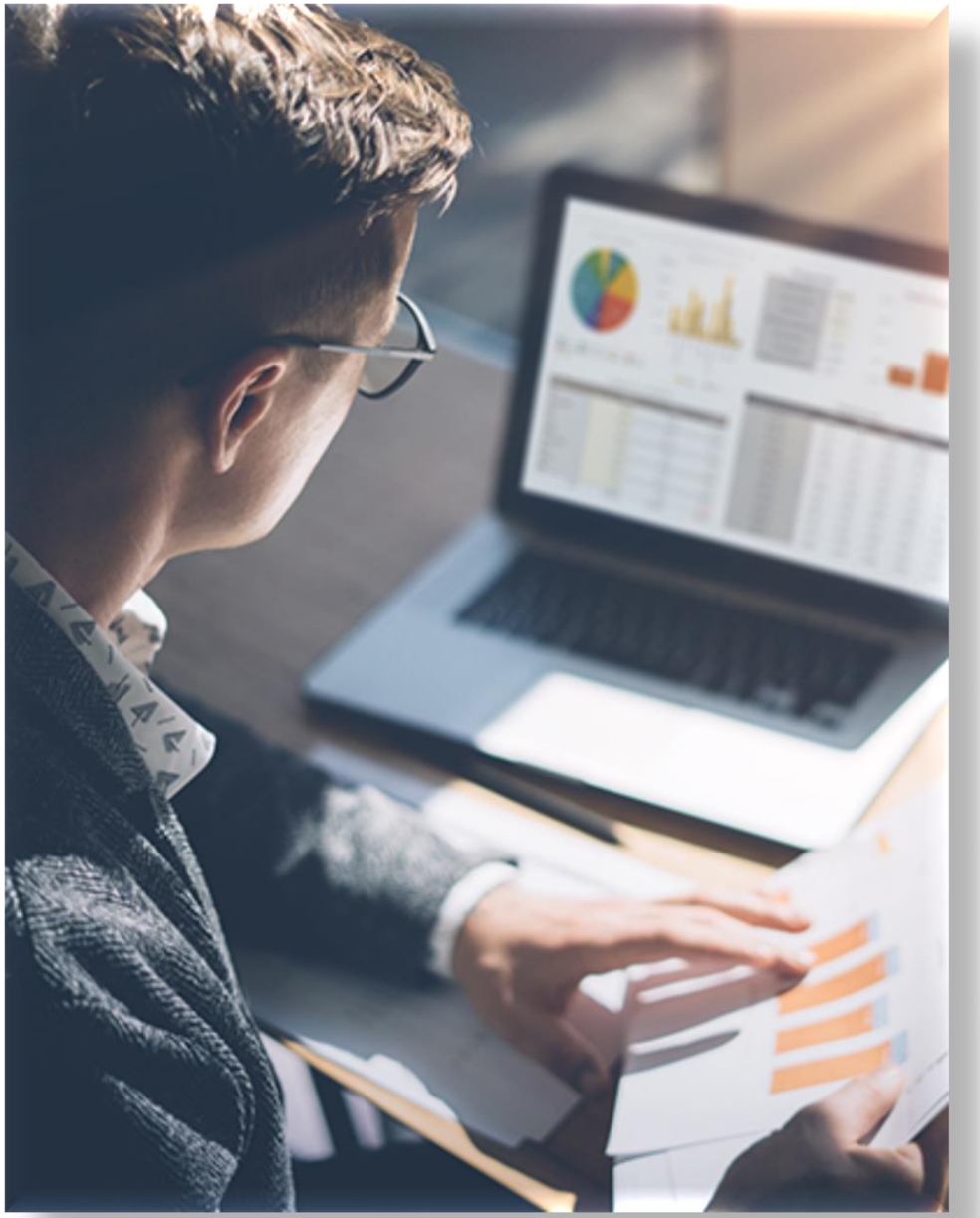
10. Risk Tolerance and Cyber Insurance

- How much cyber risk are we willing to accept?
- How much risk are we willing to transfer?
- Do we have cyber insurance?
- What are the limitations and requirements?
- Vendor and subcontractor requirements?
- Scales with VRM risk prioritization
- Is our cyber insurance coverage adequate and current to cover all costs associated with a:
  - Multi-day network outage
  - Breach mitigation and recovery
  - Lost revenue
  - Reputational harm
  - Legal and regulatory exposure
  - Victim and patient services – credit monitoring
- Forensics firms panel – integration with IRP
- Interaction and integration with other insurance policies
- Ransomware coverage – bitcoin
- “Act of war” exemption for cyber?



11. Incident Response Plan

- Do we have a **unified** cyber-incident response plan & is it up to date?
- Multi-day impact and multi-incident plan?
- Does it include specific individuals from all clinical, business, admin and facilities functions - with defined roles, responsibilities and ***off hours contact information and plan access?***
- Activation and decision escalation protocol and matrices?
- Leadership role
- Is the plan regularly tested, gaps and best practices identified and updated to include current threat scenarios such as ransomware?
- Legal, regulatory, financial and reputational risks?
- Internal and external communications strategy?
- Out of band communications
- Paper copies and downtime procedures?
- Continuity of operations – emergency management
- Cyber insurance requirements – forensics firm
- FBI, government and forensics firm integration?



12. Independent Review

Has an independent and objective outside expert reviewed, identified gaps, validated and made recommendations in each of the above areas?

- Help translate and bridge communication, organizational and political gap between technical and non technical leadership
- Outside voice and perspective
- Advocate for priorities, validation
- Immune from internal politics and dynamics
- Speak truth to power

Learning Outcomes

- Cybersecurity is not just an IT issue focused on risk to the security and privacy of patient data – It is a vendor and enterprise risk management issue.
- The cybersecurity culture of the organization – the people, are best defense or weakest link, and the most cost effective defensive measure.
- Money can't cure reputational harm and cybersecurity is a good for business
- Cybersecurity risk is constantly evolving, outpacing defensive measures and can never be eliminated, only mitigated.
- Therefore, threat detection, time to detection from intrusion, incident response and recovery plans are critical.

Learning Outcomes

- Understand that your organization may have embedded or hidden cyber risk exposure through your vendor and client relationships.
- Know your risk profile, have a constantly evolving cybersecurity strategy and execution roadmap to counter your evolving threats.
- All cybersecurity issues should be first viewed, prioritized and measured within the context of **impact to care delivery and patient safety first!**

Awareness + Collaboration + Preparedness = Confidence

John Riggi, Strategic Advisor for Cybersecurity and Risk

Advisory services uniquely informed by:

- Extensive and varied FBI and CIA experience
- Trusted and confidential access to the nation's hospital leaders
- Ongoing exchange with federal law enforcement, intelligence and regulatory agencies

jriggi@aha.org (O) 202-626-2272; (M) 24/7 202-640-9159

John Riggi, having spent nearly 30 years as a highly decorated veteran of the FBI, serves as the first Senior Advisor for Cybersecurity and Risk for the American Hospital Association (AHA) and their 5000+ member hospitals. In this role, John serves as a national resource to assist members defend against cyber attacks and other threats to their organizations. While at the FBI, John served as a representative to the White House Cyber Response Group. He also led the FBI Cyber national outreach program to develop mission critical, investigative and information sharing partnerships with the healthcare and other critical infrastructure sectors. John held a national strategic role in the FBI investigation of the largest cyber-attacks targeting healthcare and other critical infrastructure.

In coordination with the FBI and other government agencies, John is currently leading an AHA national campaign to advise members on threats to intellectual property, including nation state sponsored theft of medical research and innovation. He currently co-leads a national HHS/healthcare sector task group to develop resources to assist the field in translating cyber risk into enterprise risk. John serves as an official private sector validator for the White House's Presidential Policy Directive (PPD)-41 on U.S. Cyber Incident Coordination, to improve coordination among government agencies and cooperation with the private sector.

Previously in his career, John served in leadership positions in the FBI's Washington Office Intelligence Division, New York Office Joint Terrorist Task Force, and High Intensity Financial Crimes Area Task Force. He also served as the National Operations Manager for the FBI's Terrorist Financing Operations Section, a senior FBI representative to the CIA's Counterterrorism Center and served on the New York FBI SWAT Team for eight years. John is the recipient of the FBI Director's Award for Special Achievement in Counterterrorism and the recipient of the CIA George H.W. Bush Award for Excellence in Counterterrorism, the CIA's highest counterterrorism award. John presents extensively on cybersecurity and risk topics and is frequently interviewed by the media on cybersecurity issues.

AHA Membership Includes: