American Hospital Association™

Advancing Health in America

What's Your Cyber Risk Profile? 12 Considerations for CEOs

Cybersecurity vulnerabilities and intrusions pose risks to every hospital. While there are significant benefits for care delivery and organizational efficiency from the expanded use of networked technology and electronic exchange of health information, this greater connectivity increases exposure to potential cybersecurity threats. One of the most important things a CEO can do is to ask the right questions of their team. Here are 12 considerations you can use to start conversations across your organization.

1 Patient safety and mission critical systems: What are our most mission-critical systems, devices and networks related to patient safety and care delivery, and how vulnerable are they to cyberattacks? Have we mapped our network, our data and baseline network activity? What are our most valuable data sets, including intellectual property and research? Where are they stored, and who has access to them?

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? Who is coming after us (e.g., nation states, criminal organizations, insiders or a combination)? Why and how?

3 Tactical cyber risk profile: What is our current state tactical cyber risk profile, based on our latest risk assessments of our policies, procedures and controls, and vulnerability and penetration testing of our technical environment?

4 Prioritization: Do we prioritize all cybersecurity policies, procedures, controls and technical risks through the lens of impact to patient safety and delivery of care first; protection of patient data security and privacy second; and business and administrative operations third?

5 Capabilities: 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 information-security program? Does the reporting structure for the chief information security officer provide sufficient status, authority and independence?

6 Vendor risk-management program: Have we conducted a recent in-depth technical, legal, policy and procedural review of our vendor risk-management program to identify domestic and foreign high-risk vendors based on access to sensitive data, networks, systems, locations and criticality to continuity of operations?

AHA CENTER FOR HEALTH INNOVATION

For more information on the AHA's cybersecurity initiatives, vist: htpps://aha.org/center/cybersecurity-and-risk-advisory-services

American Hospital Association™

Advancing Health in America

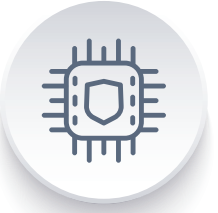
What's Your Cyber Risk Profile? 12 Considerations for CEOs

7 Cybersecurity culture: What is the cybersecurity culture of our organization? Knowing that the people of the organization represent the best defense against cyberthreats or the greatest vulnerability, do we have a proactive, top-down culture of cybersecurity in which every leader and staff member believes he or she has a duty, a role and the power to defend patients against cyberthreats? Or, is our culture of cybersecurity one that is based on compliance and data protection?

8 Risk mitigation strategy and ERM: Based on our overall current cyber risk profile, culture of cybersecurity and our target risk profile, what is our cyber risk mitigation strategy? Is it integrated into an overall multidisciplinary, enterprise risk-management program and governance structure? Do we follow a particular cybersecurity framework? Why or why not?

9 Risk mitigation implementation plan: What is our cyber risk mitigation strategy implementation road map? Are there specific program objectives and milestones along with a cost/risk-reduction analysis and patient safety impact review for each objective?

10 Incident response plan: Is our cyber-incident response plan up to date? Does it include specific individuals from all clinical and business functions and risk committees, with defined roles, responsibilities and contact information? Is the plan regularly tested, gaps and best practices identified and updated to include current threat scenarios such as ransomware? Is the FBI integrated into the plan?



11 Cyber insurance: Is our cyber insurance coverage adequate and current to cover all costs associated with a multi-day network outage, breach mitigation and recovery, reputational harm, legal and regulatory exposure?

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

John Riggi, having spent nearly 30 years as a highly decorated veteran of the FBI, serves as the senior advisor for cybersecurity and risk for the American Hospital Association and its 5,000+ member hospitals. John is available to assist your organization in conducting an in depth cyber risk profile and provide other cybersecurity advisory services such as risk mitigation strategies, vendor review and customized education and training for executives and boards.

AHA CENTER FOR HEALTH INNOVATION

You can reach John anytime at:
(O) 202-626-2272 | (M) 202-640-9159 | jriggi@aha.org