Sponsored by:

accenture

AHA TRANSFORMATION TALKS

STRATEGIES FOR REIMAGINING HEALTH CARE

Cybersecurity: Embracing a Leadership Imperative

Health care is under attackby professionals as never before and the stakes are rising for hospitals and patient safety. The latest potential threat: The FBI warns that Russia's invasion of Ukraine, which has involved cyberattacks on the Ukrainian government and critical infrastructure organizations, could impact others beyond the region, including the U.S.

This contributes to the overall enhanced threat environment under which hospitals and health systems operate today, both directly and through mission-critical third parties.

Malware and ransomware attacks as well as data breaches increasingly are putting care delivery, patients' protected health information and safety at risk. Department of Health & Human Services data from 2021 tell the story.

- More than **550 health care organizations** suffered a data breach as of the fourth quarter 2021.
- A report from the Ponemon Institute in September 2021 shows a **strong positive correlation between ransomware attacks and negative patient outcomes**.

Today, it is critical to view cybersecurity as a patient safety, enterprise-risk and strategic priority. Cybersecurity must be built into each hospital's enterprise risk-management, governance and business continuity framework.

The leadership team's ongoing commitment to this effort is imperative. Cybersecurity and patient safety initiatives must be aligned to help organizations safeguard patients and their privacy. Integrated business continuity plans should ensure that all essential functions can be sustained for at least a month after a cybersecurity attack.

As health care technology and the ways devices are deployed continue to grow, we can expect more significant data breaches, malware and ransomware attacks in the field as threat actors take advantage of new attack opportunities. In this environment, it will be critical for health systems to understand the effectiveness of the security controls they have in place and what that means for their risk profiles. Ultimately, protecting health care organizations from cyberthreats will require an end-to-end, coordinated approach that addresses the entire ecosystem.

Health care senior leaders must view cyber-risk as part of enterprise risk and bridge any gaps between information security and enterprise risk-management efforts. Hospital and health system leaders also need to work closely with their boards to define responsibilities in an effort to effectively manage cyber- and enterprise risks.

6 questions to establish baseline cyber- and enterprise-risk management

1. In your organization, is cyber-risk ranked as an enterprise risk? If so, is it ranked in the top five? Top three?
2. How often is cybersecurity briefed to the board?
3. What board committee has oversight and how is it engaged?
4. Is cybersecurity measured as a percentage of the information technology budget or the enterprise budget?
5. Is there a methodology to quantify the organization's strategic cyber-risk profile and align cybersecurity resources and budgets based on the risk?
6. Do you prioritize all strategic cyberthreats and risk-mitigation controls by their impact on:
   - Care delivery and patient safety.
   - Reputation.
   - Mission-critical operations.
   - Confidence of patients, staff, community and investors.
   - Data protection and privacy, including health records, personal health information, financial and payment data and intellectual property.
   - Revenue.
   - Legal and regulatory exposure.
   - Mergers and acquisitions.
   - Strategic business risk.

For the latest updates on Russian cybersecurity threats and resourcesin preventing and responding to cyberthreats, visit the AHA cybersecurity webpage
https://www.aha.org/cybersecurity

Discussion Questions:

1. **How has Russia's invasion of Ukraine and the associated cyberthreats created risk for U.S. health care providers?**
2. **Given the current threat environment, what should health care leaders be focusing on?**
3. **What are the essential components of an integrated business continuity plan to ensure sustained operations for at least four weeks in the event of a cyberattack?**
4. **What are some best practices for selecting a platform partner?**