Trustee Insights

CYBERSECURITY

Cybersecurity as a Clinical and Governance Imperative

A Trustee's Guide to Cyber Resilience in Health Care

BY: AJAY K. GUPTA

As technological systems play a central role in clinical care, cybersecurity has evolved from a back-office IT issue into a frontline concern for hospitals and health systems as well as their boards. Trustees must understand that cyber threats can disrupt care, endanger patient safety and damage the very mission of their organizations. This article outlines what health care trustees should know and do to ensure their organizations are resilient, responsive and ready to protect their mission in the face of cyber threats.

Effective oversight requires visibility through regular updates from staff or leadership in the following areas:

- Overall cyber risk posture along with industry benchmarking.
- Status of incident response plans and breach simulations.
- Readiness of clinical and operational systems to maintain continuity of care.
- Backup and system recovery protocols.
- Adequacy and scope of cyber insurance coverage.
- Risks from third-party vendors and service providers.
- Compliance with HIPAA, HITECH and other regulatory requirements.
- Strategic IT and cybersecurity investments and their alignment with care delivery.
- Post-incident debriefs, root causes and remediation plans.

With the right questions and insights, trustees can help foster a culture of resilience that protects patients, supports leadership and preserves public trust.

A Trustee's Guide to Cyber Resilience in Health Care

Given the role that technology infrastructure plays in supporting clinical care delivery tools, from EHR systems to networked medical devices, wearables and sensors, cybersecurity is no longer just an IT issue. It is a critical component of clinical safety, operational continuity, financial stability and organizational trust.

Recent studies show the devastating impact cyberattacks are having on patient care. Research indicates that ransomware attacks can lead to a 35% to 41% increase in patient mortality, 70% of hospitals reported increases in average length of stay and 36% of health care facilities report an increase in medical complications due to the ransomware attacks.

Trustees historically are conditioned to govern in ways that prevent disruptions to patient care, answer regulatory concerns and build community trust, and they must now recognize that these responsibilities include responding to data loss and system inaccessibility that can result from a cyberattack as well.

Cyber Preparedness: What Trustees Should Know Before an Incident Occurs

The foundation of cyber preparedness begins with a mindset shift: consider cybersecurity a *patient safety issue* and not only a technology concern. Preparation means asking the right questions and setting expectations that extend beyond system security to clinical and operational resilience.

Key areas of focus include:

- **Investment awareness.** Trustees must understand the scale and purpose of IT investments. Do they lead to secure, scalable and care-enhancing infrastructure?
- **Clinical continuity planning.** Can clinical teams continue delivering care if systems go offline? Is there an incident response plan that has been tested regularly?
- **Decision-making protocols.** Who decides when to shut down systems, notify patients, engage law enforcement and inform the board? Trustees must understand the governance structure during an incident.
- **External relationships.** Ensure relationships are established with cybersecurity experts, legal counsel and crisis communications professionals with experience handling cyber incidents. These partnerships must be formed *before* a breach occurs.

Operational Resilience: Evaluating Clinical Continuity in a Crisis

Cybersecurity today is about more than preventing breaches — it is also critical to ensure safe continuity of care when an attack happens. Trustees need to ensure measures for operational readiness are in place and tested. Trustees should ask questions that focus on these areas:

Continuity processes: Do clinical and administrative teams know when and how to launch backup systems and processes for critical systems like EHRs, lab systems, telemetry, etc.?

Patient care: Have we trained clinical and administrative staff on manual fallback procedures?

Response: Do we know how to leverage our cyber insurance and other response mechanisms?

While systems need to be as secure as practical, the goal isn't absolute security but rather *operational durability* under adverse conditions. Trustees must assess whether the organization can function safely when systems are compromised.

The Impact of a Breach and the Role of the Trustee

A cyber breach can take infrastructure offline, disrupting patient care, eroding public trust, potentially violating privacy laws, jeopardizing research integrity and creating legal and regulatory challenges.

Trustees must understand the full scope of their responsibilities before, during and after a breach:

- **Oversight of risk:** Boards should receive regular briefings on trends and threats affecting the sector. One resource is the Health Sector Cybersecurity Coordination Center (HC3), maintained by the U.S. Department of Health and Human Services, which regularly publishes threat briefings and alerts related to cybersecurity risks in health care.
- **Support during and after a crisis:** When an incident occurs, the board must act as a steadying force throughout the response and recovery periods, supporting leadership while ensuring that fiduciary duties, disclosure requirements, and remediation efforts are met with transparency and urgency while keeping the focus on patient care.

Board Reporting Expectations

Trustees have fiduciary duties that require informed oversight of all risks facing the institution. This now includes cyber risk. Regular reporting from hospital leadership should include:

- **Technology investment:** Spending on IT infrastructure and cybersecurity, future investment plans and assessment of ROI. This should include the status of backup and recovery systems as well as redundancies for patient-facing clinical systems
- **Overall cyber risk posture:** Threat landscape, internal and external (if any) risk assessments results, and benchmarking against industry standards.
- **Incident response readiness:** Status of planning, frequency and outcomes of drills, and clarity on decision-making authority during a crisis.
- **Third-party risk:** Identification of high-risk vendors and any recent issues they may have experienced.

Regulatory compliance: HIPAA/HITECH status, audit findings and disclosure readiness.

- **Cyber insurance:** Coverage levels, exclusions and whether the policy is adequate for likely scenarios.
- **Post-incident debriefs (as needed):** Detailed reporting on

actual or near-miss incidents, root cause, response performance and remediation.

These updates provide the board a view into not just security, but also whether the hospital can *function safely* during a cyber crisis. They should be detailed enough to indicate the level of confidence management has in current security and resilience measures, as well as allow the board to be able to support leadership through complex incidents.

Stewarding Cyber Resilience at the Board Level

The most important message for health care trustees is this: **Cybersecurity is a governance responsibility.**

In the era of digital health, cybersecurity is no longer just an IT concern, it is a clinical and governance imperative. Technology infrastructure now directly impacts patient safety, operational continuity and a health system's ability to fulfill its mission.

Just as boards oversee financial health and care quality, they must now also oversee cyber resilience, ensuring leadership has strong defense and recovery plans that are developed and communicated.

Effective governance requires more than understanding risk; it demands consistent visibility into how risk is being managed. Board-level oversight, through asking the right questions, supporting strategic investments and maintaining organizational readiness, is essential to building a culture of preparedness that protects patients, preserves public trust and sustains mission-driven care.

Cyber threats are now capable of disrupting care and endangering lives. Trustees must lead with urgency, foresight and resolve, and in doing so, they can ensure their institutions are equipped to withstand cyber attacks and emerge stronger.

Ajay K. Gupta (agupta@healthsolutionsresearch.org) is co-founder and CEO, HSR.health, and Inaugural Board Chair for Trinity Health Mid-Atlantic and Holy Cross Health.

Please note that the views of authors do not always reflect the views of the AHA.