Kentucky Trustee

For Kentucky Hospital Governing Board Members Spring 2025

BOARDROOM BASICS

Cybersecurity: Boards Must Prepare for an Increase in Number and Scale of Attacks

While all industries are impacted by cyber attacks, the health care industry stands out. Health care is the most attacked industry, and once those attacks occur the impact grows as it affects quality of patient care, hospital financial viability, and individual patient lives.

Every hospital and health system should be simultaneously taking action to prevent a cyberattack and practicing responses to potential cyberattack scenarios. The number and severity of attacks is increasing, and it is impacting all organizations—large and small—across the globe.

In November 2024, the World Health Organization (WHO) Director-General Tedros Adhanom Ghebreyesus discussed the importance of global cyberattacks at a UN Security Council meeting. He called for global action to address the cybersecurity crisis, saying that: "**Ransomware and other cyberattacks on hospitals and other health facilities are not just issues of security and confidentiality, they can be issues of life and death**…at best, these attacks cause disruption and financial loss. At worst, they undermine trust in the health systems on which people depend, and even cause patient harm and death."[1]

Attacks are Increasing

Health care is the most attacked industry because of the opportunities it presents to cyberattackers. Hackers have access to large numbers of personal data, which can be sold, held for ransom, or both. When systems are shut down the impact is so significant that health care organizations are highly motivated to end the lockdown quickly.

2024 set a record for the highest number of cyberattacks in the health care industry, and the outlook is grim. Experts predict the number and scale of attacks will get worse, particularly as hacks are driven by artificial intelligence.[2]

Ransomware. Ransomware attacks are when a hacker locks down all data and systems, and offer to "turn it all back on" once a ransom is paid. The ransom is usually requested in a cryptocurrency because it is hard to trace. The attackers also encrypt backup systems so that backup data is not available without payment. These attacks are becoming more complex and widespread, and the time it takes for health care organizations to recover is taking longer.

When they are attacked, not all organizations share publicly if they paid the ransom and how much they paid. One survey reported that in 2024 the average ransom paid was $4 million.[2] Unfortunately, the ransom is

Kentucky Hospital Association
2501 Nelson Miller Parkway Louisville, Kentucky 40223 TEL: 502-426-6220 FAX: 502-426-6226 www.kyha.com

PRESIDENT'S NOTEBOOK

Nancy Galvagni
President and CEO

The KHA team is busy this spring on multiple fronts and I have two exciting announcements to share with you.

First, KHA has launched a media campaign designed to promote the health care field to middle and high school students. The campaign, "Put Me in Coach" includes commercials and ads on social media and television encouraging young people to explore future opportunities in Kentucky hospitals.

The upcoming and newest generation is motivated to help their communities. They have the mission and want the opportunity to join a team that makes a true difference to improve people's lives – their friends and families. Hospitals provide that exact mission and opportunity, offering a variety of rewarding careers that truly make a community difference.

Stay tuned for more news on this exciting new campaign.

Second, we were honored by *Modern Healthcare* magazine with a 2025 Innovators Award! The award celebrates both outstanding individuals and organizations leading health care innovation. Detailed profiles of all the honorees were featured in the April 14, 2025, issue of *Modern Healthcare* magazine and online at ModernHealthcare.com/Innovators-Org.

Modern Healthcare's Innovators program recognizes leaders and organizations driving innovation that improves care, achieves measurable results, and contributes to the clinical and financial goals of the organization. KHA was recognized for creating and supporting the Hospital Rate Improvement Program, a value-based program allowing the state to earn more federal funds for improving health care quality.

If you ever need help on any issues impacting your hospital or system, please feel free to reach out to me or the rest of the KHA staff. We are here to serve you!

Sincerely,

Nancy Galvagni
President and CEO
Kentucky Hospital Association

Governance Notebook

Mark Your Calendars: Upcoming KHA Events

Mid-South Critical Access and Rural Hospital Conference – August 20-21, 2025
Louisville, KY

KHA Health Policy Conference – October 16, 2025
Lexington, KY

Fall Health Care Workforce Summit – November 2025
Louisville, KY

KHA 97th Annual Convention – May 2026
Louisville, KY

Do you have ideas for future issues of the *Kentucky Trustee*?

Our goal is to provide you with the information and knowledge you need to lead your hospitals forward in today's rapidly changing environment. Tell us what you think, and what you would like to see in future issues of the *Kentucky Trustee.*

Write or call:
Ginger Dreyer
Kentucky Hospital Association
2501 Nelson Miller Parkway
Louisville, KY 40223
502-426-6220 or 800-945-4542
gdreyer@kyha.com

only the start of the cost. Even when organizations get their data back, they spend millions in recovery costs and the recovery process takes time. In 2023, 28% of health care organizations said it took a month to recover from a ransomware attack. In 2024, 37% said it took more than a month to recover.[2]

Data Breaches. A data breach occurs anytime there is unauthorized access to patient data. Unlike ransomware with the goal of receiving a payment, data breaches are about stealing patient information and selling or publishing it.

Health care organizations have experienced a decline in the number of data breaches, but the total number of records breached has increased because the size and scope of the attacks have increased. In total, there were 14 data breaches in 2024 that involved more than 1 million health care records. Just those 14 breaches resulted in exposed or compromised data of about 70 percent of the U.S. population.[2]

The Impact of a Cyberattack

The impact of a cyberattack is an immediate threat to patient care, potentially shutting down systems that provide vital information and either disrupt, delay, or completely cancel patient care. The American Hospital Association (AHA) describes cyber threats such as ransomware attacks as "threat-to-life crimes" because of the potential patient safety risk to anyone depending on the hospital in an emergency.[5] In addition, cyberattacks can create long-term delays in patient care or divert patients to other facilities for treatment. Attacks also have the potential to negatively impact hospital goodwill and result in lawsuits due to inadequate preparations by the hospital.

Recent Examples

Cyberattacks impact organizations of all sizes. While the Change Healthcare attack was the most high profile cyberattack in 2024, brief overviews of a few recent attacks paint a clear picture of the depth of the risk hospitals and health systems face.

Change Healthcare. In February 2024 a Russian ransomware group attacked Change Healthcare, a subsidiary of UnitedHealth Group. The ransomware attack sent ripples throughout the health care industry that lasted for months.

The chaos it created included doctors' inability to look up patient medical histories, pharmacies not verifying prescriptions, problems with billing and insurance approvals, and more.[3]

Overall, the attack impacted 190 million people. 74 percent of hospitals reported a direct impact on patient care, and 94 percent reported that the attack impacted them financially. One third of hospitals reported that the attack disrupted more than half of their revenue.[4]

In 2024, 37% of health care organizations said it took more than a month to recover from a ransomware attack.[2]

Ascension. In May 2024 Ascension, a St. Louis-based nonprofit health system, experienced a ransomware attack that impacted 140 hospitals across multiple states. Caregivers working during the attack reported concerns about medical errors and delays impacting patient care.[5]

Eduardo Conrado, President of Ascension, described the impact the attack had on patient care: "Nurses were unable to look up patient records from their computer stations and were forced to comb through paper back-ups…imaging teams were unable to quickly send the latest scans up to surgeons waiting in the operating rooms, and we had to rely on runners to deliver printed copies of the scans to the hands of our surgery teams."[1]

It took 37 days for Ascension to restore operations. The health system reported the cost of response and recovery was $130 million, and that it lost $0.9 billion in operating revenue.[1]

American Hospital Association: Change Healthcare Attack Lessons Learned

In February 2024 a Russian ransomware group attacked Change Healthcare, a subsidiary of UnitedHealth Group. The attack directly impacted patient care and hospital finances, disrupting revenue and impacting operations for months after the attack. The records of 190 million Americans were impacted, and the American Hospital Association (AHA) reports that every hospital in the country was either directly or indirectly impacted.

In 2025 the AHA released a report summarizing the impact and implications for hospitals and health systems. Below is an overview of the report's lessons learned. For the full report, go to www.aha.org/cybersecurity.

Third-Party Cyber Risk is the Most Significant Threat to Health Care. Cyber attacks want to maximize disruption to care delivery, often causing delays to care that impact patient safety, particularly in emergency situations. The vast majority of cyber attacks in 2023 and 2024 were through business associates, third parties, health plans and non-hospital health care providers. To prevent cyber attacks, hospitals and health systems must have a third-party risk management program that:

- Identifies and prioritizes risks posed by third-party vendors and subcontractors
- Incorporates third-party risk-based controls and cyber insurance requirements
- Consistently communicates these risk management policies internally

An Immediate, Coordinated Response is Essential. When the Change Healthcare attack occurred, no one knew how far the impacts would reach. Hospitals were unclear about the federal government's responsibility to step in, and CMS had limited authority to help. Prevention and response when attacks do occur must involve multiple stakeholders, including government partners.

Plans Should Ensure Clinical and Business Continuity for at Least 30 Days. Hospitals must be able to provide care without core technology systems for four weeks or longer. This requires:

- Enhancing clinical, operational and financial downtime and backup processes
- Training all staff in manual procedures necessary to continue operations and care delivery
- Ensuring plans align with the Department of Health and Human Services voluntary Cybersecurity Performance Goals
- Working with regional stakeholders on response and recovery plans

Hospitals must be able to provide care without core technology systems for four weeks or longer.

Strategic Considerations. The merger of UnitedHealth Group (UHG), Change Healthcare and Optum led to many hospitals and health systems becoming overdependent on one organization's services. Despite this, most health care organizations did not identify their dependency on UHG/Change Healthcare as a risk. The attack highlights the importance of health care organizations having diversification and redundancy in their mission-critical service providers.

Source: Change Healthcare Cyberattack Underscores Urgent Need to Strengthen Cyber Preparedness for Individual Health Care Organizations and as a Field. American Hospital Association. January 2025.

These ransomware attacks are not data crimes, but life-threatening violent crimes. The ransom demand is in fact an extortion based upon the risk to patient safety.
- John Riggi, the AHA National Advisor for Cybersecurity and Risk

Fred Hutchinson Cancer Center. In November 2023 Fred Hutchinson Cancer Center in Seattle, WA experienced a "double ransomware" attack. When the Cancer Center didn't pay the ransom demanded, the hackers began contacting patients directly. They sent individual patients a link to where the information was "on sale," and asked for $50 in bitcoin to take it down. In some cases, patients received additional threats, including reporting them to law enforcement.[6]

McKenzie Health System. In March 2022, McKenzie Health System, a Critical Access Hospital in Michigan, experienced a cyberattack. The attack likely began with a phishing email that got through the hospital's spam software.[7]

Once all electronic systems were locked, the hospital transitioned to paper systems. Because of its rural nature and the technology interruptions they had previously experienced, the hospital had practiced providing technology-free care before. Still, the attack took a toll as it dragged on.[7]

The cyberattackers demanded a 7-figure ransom to prevent the release of personal information on the dark web, and ultimately the hospital decided not to pay the ransom.[7]

Before the attack, the hospital had prepared: they had cybersecurity insurance, had engaged a disaster recovery organization, and had redundancy in their IT system. The remote server backups occurring every 12 hours helped in the recovery. Four months after the attack, the hospital reported still working with the disaster recovery team to respond to the attack and better prepare for the future.[7]

Hospitals Must Prepare for Multiple Scenarios

Cyberattackers can infiltrate hospital systems through a variety of methods, such as malware or phishing attacks. Another challenge is through third-party vendors.

After initial shock and recovery from the Change Healthcare attack, the AHA developed a summary report with lessons learned. One of the primary findings was that the greatest risk for hospitals and health systems is through third party breaches, including associates, third parties, health plans, and non-hospital health care providers. Attackers use a "hub and spoke" strategy where they attack the hub (the third party technology), which then gives them access to all the spokes. Each health care organization that uses the third-party provider is one of the spokes.[4]

Change Healthcare touches one in every three patient records, making it an ideal "hub" for reaching lots of spokes.

The greatest risk for hospitals and health systems is through third party breaches.

John Riggi, the AHA National Advisor for Cybersecurity and Risk, explained: "If there was ever any question that the intent of these gangs was to harm patients, it is clear now that it is their fundamental intent. These ransomware attacks are not data crimes, but life-threatening violent crimes. The ransom demand is in fact an extortion based upon the risk to patient safety."[4]

Rural Hospitals Face Bigger Cybersecurity Challenges

Rural hospitals are not immune to cybersecurity attacks and there have been multiple data breaches and cyberattacks on small hospitals in the last five years. Although the ripples created across the nation may not be the

same as a large health system, experts agree that rural hospitals and health systems are particularly at risk. Finding information technology (IT) professionals can be difficult in rural communities. In addition, high-end cybersecurity systems are primarily marketed to large health care organizations that can afford the cost.[5]

According to a recent Microsoft report on cybersecurity, hospitals lose $1.9 million per day of downtime during an attack. For rural hospitals, this impact can be devastating.[9]

Experts agree that rural hospitals and health systems are particularly at risk for a cybersecurity attack.

The U.S. Department of Health and Human Services (HHS) has set cybersecurity performance goals for hospitals and health systems, but many rural hospitals do not have the resources to meet the goals. In Spring 2024 the AHA and Microsoft partnered to create the Microsoft Cybersecurity Program for Rural Hospitals to help small and rural hospitals access the training, resources, and products necessary to be more prepared. More information about the program is available at www.aha.org/cybersecurity.[10]

What Boards Can Do

Cybersecurity is a strategic issue for hospitals and health systems. Boards must proactively take action to both protect their hospital from an attack and to have a plan in place if an attack does occur.

Include Cybersecurity in Risk Management Oversight. Cybersecurity should be part of every hospital's enterprise risk management (ERM) approach. The board should understand the basics of cybersecurity, how it fits into the ERM framework, and receive regular updates.

Review Cybersecurity Insurance. Cyber insurance should be part of the hospital's ERM strategy. It can include coverage when an attack occurs, data recovery, consultations if an attack occurs, and experts who negotiate with attackers real-time. Boards should regularly review their cybersecurity coverage to see if adjustments need to be made.

Engage in Board Education. Boards must prioritize high-level education about cybersecurity risks and the board's role in mitigating the risks.

Provide Adequate Support. The board sets the tone for the importance of cybersecurity by ensuring adequate resources are allocated. This might include funding for staffing, technology upgrades, organization-wide training and education, increased security procedures, and emergency management drills to prepare for a potential attack.

Ensure Cybersecurity Talent. All hospitals and health systems should have a cybersecurity expert working at the highest level within the organization. This might require external recruitment or training existing talent within the organization. Leaders should also be filling the pipeline with future talent that can respond to the ever-evolving challenges in the cybersecurity world.

Assign a Cybersecurity Expert. Security is more likely to be effective if someone "owns" cybersecurity within the organization's leadership team. This might be a Chief Security Officer, Chief Privacy Officer or Compliance Officer. Typically this expert would report to the full board or the assigned board committee.

Consider Delegating Cybersecurity to a Board Committee. Assigning

Cyberattack Statistics

$9.77 million

The average cost of a health care data breach in the U.S. in 2024 [8]

$1.9 million

The amount hospitals lose per day for each day of downtime after a ransomware attack [9]

$4 million

The average ransom paid for a ransomware attack, which does not include recovery costs [2]

150 million

The number of American health care records hacked in America in 2024 [8]

85%

Of the largest health care data breaches are due to attacks on third-party providers or non-hospital organizations [8]

HHS Cybersecurity Performance Goals

HHS has published voluntary Cybersecurity Performance Goals specific to health care organizations. The guidelines include "essential goals" and "enhanced goals." The essential goals include:[11]

- Mitigate known vulnerabilities
- Email security
- Multifactor authentication
- Basic cybersecurity training
- Strong encryption
- Revoke credentials for departing workforce members
- Basic incident planning and preparedness
- Unique credentials
- Separate user and privileged accounts
- Vendor/supplier cybersecurity requirements

Boards do not need to know the micro details of each goal, but they should prioritize the importance of meeting essential goals, including funding and receiving regular updates on progress.

cybersecurity to a board committee can provide more detailed oversight and governance. The assigned committee should oversee potential risks and exposures, set goals for addressing those risks, and regularly review progress.

Questions for Boards to Consider

Proper governance education and regular reporting to the board gives board members opportunities to ask informed questions about the hospital's cybersecurity strategies. Boards should ask questions such as:

- Is cybersecurity part of our organization's enterprise risk management thinking?
- Is our insurance coverage adequate?
- Do we have sufficient cybersecurity expertise at our organization?
- Does our organization have a team reviewing and implementing cybersecurity plans related to the HHS voluntary Cybersecurity Performance Goals?
- Are we working with experts to ensure adequate data back-up and recoverability?
- Are we providing regular staff training to minimize the potential for human error that leads to a cyber attack?
- Do we know who our mission-critical third party providers are? Where could our hospital be a spoke in a "hub" that is attacked?
- Could our hospital or health system provide mission-critical care for 30 days without core technology systems? If not, what steps should be taken to work toward this goal?
- Have we conducted disaster planning drills for a cybersecurity attack?

Sources and More Information

1. Mishra, V. Cyberattacks on Healthcare: A Global Threat that Can't Be Ignored. *United Nations, UN News*. Nov. 8, 2024.
2. Alder, S. Healthcare Ransomware Attacks Continue to Increase in Number and Severity. *HIPAA Journal*. Sept. 30, 2024.
3. Minemyer, P. UnitedHealth Estimates 190M People Impacted by Change Healthcare Cyberattack. *Fierce Healthcare*. January 24, 2025.
4. Change Healthcare Cyberattack Underscores Urgent Need to Strengthen Cyber Preparedness for Individual Health Care Organizations and as a Field. *American Hospital Association*. January 2025.
5. Bolton, A. After Health Care Attacks, Tech Giants will Help Small Hospitals with Cyber Defenses. *National Public Radio*. August 14, 2024.
6. Blum, K. When Hospital Ransomware Attacks Target Patients: A New Trend to Follow. *Association of Health Care Journalists*. January 30, 2024.
7. An Unseen Threat Actor Attacks a Critical Access Hospital's Digital Network in Sandusky, Michigan. *Rural Health Information Hub*. November 14, 2022.
8. 2025 Environmental Scan. *American Hospital Association*. www.aha.org/environmentalscan.
9. Southwick, R. Ransomware Attacks Threaten Rural Hospitals | HIMSS 2025. *Chief Healthcare Executive*. March 6, 2025.
10. Riggi, J. Resources to Protect America's Rural Hospitals from Cyberthreats. *American Hospital Association Cybersecurity Blog*. February 18, 2025.
11. HPH Cybersecurity Performance Goals. *Health and Human Services*. Accessed April 3, 2025. https://hhscyber.hhs.gov/performance-goals.html.
12. Baviskar, N. Cybersecurity Awareness is a Board Responsibility. *AHA Trustee Services*. Accessed April 3, 2025.

GOVERNANCE INSIGHTS

Ensuring Meaningful Mission, Vision and Values

Too often hospital leaders develop mission, vision and values statements, and then don't make meaningful strategic use of these critical statements.

Successful governing boards know that these statements, when properly developed and used, are the primary driver for every governance discussion and decision.

The Basics

The mission is the core purpose of the hospital. It should be a unique description that clearly defines the hospital's distinctiveness and differentiation. Great mission statements are short, memorable, highly focused and enduring. They are easily memorizable and used as a guiding light for decisions made throughout the organization.

The vision is a vivid description of what the hospital or health system seeks to become in the future. Many believe that a vision should be a simple, short and concise statement. That view often leads to a very general goal that doesn't truly describe the future the hospital seeks to achieve.

Instead, a strategically usable vision is one that describes what the organization seeks to become in the future in critical organizational success areas.

Values are the principles and beliefs that drive organizational behavior at every level throughout the entire organization. Values are not simply a collection of high-sounding words on a wall in the hospital lobby. They are the "rules of the road" that signify what the hospital is and what it believes. They should be communicated and demonstrated through action – every day, in every way.

Leveraging Your Mission, Vision and Values

Keep the Mission Center. The mission, vision and values should be prominent elements of decision making at all board meetings. Not only should they be displayed with every board meeting agenda, but items should not appear on the board agenda unless they are directly connected to the mission, vision and values. When considering any decision, boards should always discuss how the decision will contribute to fulfilling the organization's mission.

Check Alignment with the Strategic Course. When considering policy and strategy decisions, boards should put them to the mission, vision and values alignment test. Do they fit? Can their rationale be explained? Is an investment in them an investment in furthering mission, vision and values success?

What Do We Know Today That We Didn't Know Then? One vital question that should be regularly asked by the board of trustees is this:

"What do we know today that we didn't know when we developed our vision for the future? And if we had known then what we know now, would our assumptions change? Would our strategies change? What would we be doing differently?"

It's important that the mission, vision and values be reviewed on a planned, predictable basis, such as at the board's annual retreat. These should not be static statements. Instead, they evolve as the environment evolves. Assumptions should be challenged, and developing realities should be factored into the hospital's thinking. The only way to ensure that occurs is through a continual flow of new information and ideas that drive new assumptions.

Seek Leadership Involvement, Particularly from the Medical Staff. Defining the hospital's mission, vision and values is not the exclusive job of the board. It's one of the primary responsibilities of the board, but to do it right requires involvement and buy-in across the organization.

The medical staff is one of the principal groups whose input and involvement is critical to success. In addition, the board should always depend on well thought-out options and alternatives from management to help shape the mission, vision and values course.