HIMSS®
GLOBAL HEALTH CONFERENCE
& EXHIBITION

Reflections From the Frontlines of Health Innovation: Healthcare Cybersecurity

A Conversation with HIMSS25 Speakers

CONTENTS

CONTRIBUTORS

Greg Garcia
Executive Director
Health Sector Coordinating Council Cybersecurity Working Group

Anahi Santiago
Chief Information Security Officer
Christiana Care Health System

Randy Yates
Vice President and Chief Information Security Officer
Memorial Hermann Health

INTRODUCTION

Critical systems demand collective defense.

Healthcare cybersecurity has moved from theoretical risk to systemic reality. The February 2024 Change Healthcare ransomware attack - which disrupted one-third of the nation's healthcare prescriptions and reimbursements - proved that cybersecurity isn't just about protecting data; it's about preserving care delivery itself.

In modern healthcare, cybersecurity isn't just an IT function - it's a cornerstone of patient care and operational continuity.

At the HIMSS25 Healthcare Cybersecurity Forum, industry leaders confronted this new reality head-on, sharing strategies that move beyond reactive defense toward systemic resilience. Their insights reveal an industry at a critical juncture, where the integration of digital innovation and patient care demands a fundamental reimagining of how we protect healthcare's critical infrastructure.

The perspectives captured here come from leaders actively defending healthcare's digital frontier - from hospital systems and industry coalitions to technology innovators. They offer clear-eyed assessments of current vulnerabilities, practical approaches to building resilience, and strategic frameworks for securing healthcare's future. Their experiences underscore a crucial truth: in modern healthcare, cybersecurity isn't just an IT function - it's a cornerstone of patient care and operational continuity.

Whether you're mapping critical system dependencies, building cross-organizational defense strategies, or preparing for quantum computing's impact on healthcare security, these insights provide a practical roadmap for strengthening healthcare's cyber resilience - today and tomorrow.

56%

of healthcare organizations experienced delays in procedures or tests due to cyberattacks in 2024

Source: Mental Health America. (2024) DialogHealth Healthcare Cybersecurity Report

REAL-WORLD EXAMPLES
of Healthcare Cybersecurity

Operational risk meets real-time response.

Cybersecurity in healthcare is no longer a back-office issue - it's frontline infrastructure. At HIMSS25, speakers emphasized how real-world cyber events exposed the sector's most critical chokepoints. But these moments also sparked meaningful response - from new cross-sector collaboration models to contingency planning and risk-mapping frameworks.

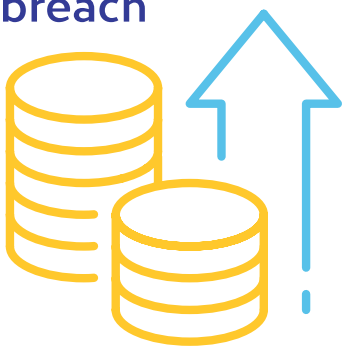
These leaders didn't speak in hypotheticals - they shared what their organizations actually did in the wake of crisis. The following responses reflect the real conditions that inspired action, the hard lessons learned under pressure, and the tangible steps being taken to harden systems and protect patients at scale.

Greg Garcia: The February 2024 Change Healthcare ransomware attack, which disrupted one-third of national healthcare prescriptions and reimbursements, exposed healthcare's critical vulnerability to cyber threats. This incident demonstrated how disruption to a single service provider can create cascading effects throughout the entire healthcare system, impacting both clinical operations and patient care. This was a real-life manifestation of systemic risk.

Anahi Santiago: The healthcare perimeter has fundamentally changed. ChristianaCare's transition to Hospital at Home and Remote Patient Monitoring initiatives has dissolved traditional hospital boundaries, creating a new cybersecurity imperative. Each patient's home has become an extension of our hospital network, dramatically expanding our threat surface and requiring us to reimagine how we protect patient data and medical devices across this distributed care ecosystem.

Randy Yates: The Change Healthcare outage had a direct impact on our pharmacy and revenue cycle operations. This service disruption prompted our organization to conduct a thorough debrief and take concrete action. We are now systematically identifying critical business functions and developing specific contingency plans to maintain operations during any extended cloud service disruptions.

The average cost of a healthcare data breach has risen to $4.88 million, with the highest breach costs occurring at critical infrastructure entities.



Source: The HIPAA Journal. (2024)

Lessons You Can Apply Now:
KEY TAKEAWAYS FROM HIMSS25

Cybersecurity isn't just about defense. It's about design.

At HIMSS25, speakers emphasized that securing healthcare systems requires more than reactive measures; it demands proactive, strategic integration of cybersecurity into every facet of healthcare operations. From workforce training to technological innovation, the focus is on building resilient systems that can anticipate and withstand cyber threats.

These insights from industry leaders highlight the critical components of effective cybersecurity strategies and offer practical steps for healthcare organizations aiming to enhance their security posture.

Greg Garcia: The healthcare system is enormously complex, with interconnected systems and dependencies that ultimately rely on the strength of the weakest link. While we operate in a heavily regulated sector, our critical vulnerability lies in our dependence on unregulated third-party technology and services - these often become our weakest link. To protect our critical healthcare infrastructure, we need to devise a comprehensive system that holds all participants accountable to appropriate security standards. This is essential given our 'critical infrastructure' designation - a status that recognizes our vital role in the nation's public health and safety, national security, and economic security.

Anahi Santiago: Innovation and cybersecurity can co-exist and thrive if cybersecurity maintains a seat at the strategic table.

Randy Yates: Cyber attacks are not a matter of if, but when. While defensive strategies should now be well-established, organizations must shift focus toward building robust detection capabilities. This means architecting sophisticated alert systems that enable rapid countermeasures - such as data center shutdowns or network segmentation - to contain and minimize attack impacts. Business owners should also implement redundancy tactics to allow for the transition of mission-critical services from one cloud service provider to another should the primary become unavailable due to attack.

> *"Innovation and cybersecurity can co-exist and thrive if cybersecurity maintains a seat at the strategic table."*
> *– Anahi Santiago*

Healthcare remains the costliest industry for data breaches, with an average cost of **$9.77 million** per incident in 2024.

Source: IBM Cost of a Data Breach Report (2024)

CHARTING THE NEXT CHAPTER
for Healthcare Cybersecurity

From reactive defense to proactive resilience.

At HIMSS25, cybersecurity leaders emphasized that the future of healthcare security hinges on proactive strategies, collaborative frameworks, and adaptive technologies. As cyber threats evolve, so too must the approaches to safeguard patient data and ensure uninterrupted care delivery.

Greg Garcia: The future of healthcare cybersecurity isn't predetermined—it's a spectrum of possibilities shaped by our collective choices. Like light through a prism, our path forward splits into different trajectories based on how industry and government invest in three critical dimensions: our people, our processes, and our technology. While we can't predict the exact future, we know the essential elements for success:

First, we must ensure cyber defense tools and resources are not just available but actionable - designed for real-world implementation and measurable impact.

Second, we must build and nurture our cybersecurity workforce through continuous training and professional development, creating both immediate capability and sustainable talent pipelines.

Third, we must drive innovation that balances digital healthcare's transformative potential with robust security frameworks, making protection an enabler rather than a barrier.

Finally, and most critically, we must embrace cybersecurity as a collective endeavor. Like a beehive or ant colony, our strength lies in unified response and shared defense. Individual excellence matters, but community resilience is paramount.

Anahi Santiago: The healthcare industry remains particularly vulnerable due to two factors: the significant disparity in organizational security maturity across the sector, and the complex challenge of protecting geographically dispersed assets. Furthermore, with Post-Quantum Computing (PQC) on the horizon, organizations must begin comprehensive planning now to effectively combat the associated threats.

Randy Yates: Developing technology resiliency plans and architectures that allow for continued use of systems that have not been impacted by a cyber-attack is crucial. For our organization, that means developing redundant endpoints and secure networks that can be brought online to make available our cloud applications and services that have not been impacted by our internal incident.

In 2023, over
167 million Americans
had their healthcare data
compromised due to cyberattacks.

Source: Reuters. (2024, December 27)

SESSION SPOTLIGHTS

From crisis response to strategic resilience.

The Healthcare Cybersecurity Forum sessions offered a practical, often hard-won look at what it takes to move healthcare cybersecurity from concept to reality. From integrating cybersecurity into organizational strategy to operationalizing contingency plans and leveraging AI responsibly in clinical settings, these conversations revealed what's working - and what still needs to evolve.

These insights from our speakers highlight key lessons from the frontlines of healthcare cybersecurity transformation.

Greg Garcia

What proactive strategies have proven most effective in anticipating and mitigating advanced cyberattacks before they impact patient care?

Several proactive strategies will help:

- Be active in information sharing and collective incident response, such as through the Health-ISAC (Health Information Sharing and Analysis Center)
- Know what you're trying to protect - your data and systems - and prioritize their value based on material risk to ensure informed investments with limited resources.
- Know your third parties and systems that you can't control, and prepare backups and continuity plans for their failure.
- Get good people and train them; cybersecurity is everyone's responsibility, just with differing roles and levels of responsibility.

How can healthcare organizations leverage risk mapping initiatives to prioritize cybersecurity investments and enhance overall resilience?

There are many critical functions and services in clinical, administrative, manufacturing, and supply chain workflows that are either invisible to all but a few specialists or simply taken for granted. If we can visualize the pathways of those services, measure and compare the disruption impact of given services, and then prioritize investments, compensating controls, and initiatives, then we will have informed risk management. It means ripping up the floorboards and examining the plumbing to see where the leaks and loose joints are before the house is flooded.

> *"[Informed risk management] means ripping up the floorboards and examining the plumbing to see where the leaks and loose joints are before the house is flooded."*
> *– Greg Garcia*

Anahi Santiago

What are some practical ways AI can simplify cybersecurity processes while enhancing organizational security?

AI can replace repetitive, low-reward tasks, freeing up cybersecurity personnel to work on more rewarding, value-added initiatives. AI can also mitigate threats faster and with more precision than humans.

Randy Yates

You emphasized the importance of collaborative support mechanisms. Can you share an example of how cross-organizational collaboration has enhanced cybersecurity resilience in your experience?

Cross-sharing of resiliency initiatives that work is helpful. We frequently share our Business Continuity strategy with peers locally and at industry-related conferences. Our emergency management team has spent three years uplifting our downtime procedure into business continuity plans that could sustain operations for 30+ days. Through real events and planned testing, many lessons learned have allowed us to continually improve the plan and make technology investments that will supplement the business continuity updates.

Only

36%

of healthcare organizations have a comprehensive cybersecurity incident response plan, highlighting a significant gap in preparedness across the sector.

Source: Market.us. (2025)

CONCLUSION

Securing Tomorrow's Healthcare: Your Call to Action

The HIMSS25 Healthcare Cybersecurity Forum illuminated a critical truth: in today's digital healthcare landscape, cybersecurity is not a peripheral concern - it's integral to patient safety and operational continuity. But the journey doesn't end here. The evolving threat landscape demands continuous vigilance, adaptation, and collaboration.

As cyber threats become more sophisticated, healthcare organizations must prioritize:

- **Strategic Investment:** Allocating resources to advanced cybersecurity technologies and infrastructure.
- **Workforce Development:** Enhancing training programs to build a skilled cybersecurity workforce
- **Collaborative Frameworks:** Engaging in cross-sector partnerships to share intelligence and best practices.
- **Regulatory Compliance:** Adhering to evolving cybersecurity regulations to protect patient data and maintain trust.

The Stakes Have Never Been Higher

- Patient lives depend on secure, reliable healthcare systems
- Cyber threats are becoming more sophisticated by the day
- Healthcare organizations face unprecedented challenges in protecting sensitive data
- The cost of inaction could be catastrophic

Be part of the next chapter in healthcare cybersecurity innovation. Join industry pioneers, thought leaders, and cybersecurity experts as we shape the future of secure healthcare delivery.