HIMSS

HEALTHCARE CYBERSECURITY FORUM

7-8 September, 2023 | **Boston**

AGENDA *(SUBJECT TO CHANGE)*

OPENING KEYNOTE: THE GLOBAL CYBER THREAT LANDSCAPE: HEALTHCARE RISK, IMPACT, AND RESPONSE

John Riggi, National Advisor for Cybersecurity and Risk, American Hospital Association

Cyber attacks against hospitals and health systems have increased dramatically with the onset of the pandemic as nation state and criminal cyber adversaries have targeted healthcare organizations with a record number of hacks. These attacks involve the theft of massive amounts of patient data and medical research. Most concerning, high impact ransomware attacks have struck hospitals and health systems at an alarming rate, causing significant disruption and delay of healthcare delivery, and risking patient safety.

Join John Riggi, National Advisor for Cybersecurity and Risk for the American Hospital Association and former FBI Cyber senior executive, as he provides his unique national and international perspective on the latest cyber threats, including those arising from geopolitical tensions and the use of artificial intelligence. John will discuss how best to prepare for, respond to, and recover from these disruptive cyber attacks. Plus, he will elaborate on the latest cyber legislative and policy developments.

PANEL: FOSTERING A SECURITY-DRIVEN CULTURE

Renee Broadbent, Chief Security Officer & Information Security Officer, SoNE Health
Christian Dameff, Medical Director of Cybersecurity, UCLA Medical
Erik Decker, VP & Chief Information Security Officer, Intermountain Health
Kelby Price, Vice President Corporate Development & Strategic Partnerships, XQ

Cybersecurity is a collective effort that requires collaboration across all levels of an organization, from stakeholder buy-in to employee awareness and accountability. This panel is designed to equip attendees with the knowledge and strategies needed to establish and maintain a strong cybersecurity culture within their organizations. Explore the critical role of leadership in setting the tone for cybersecurity practices and establishing policies and procedures to guide employees. Get proactive measures to reduce the likelihood of human error by instilling a sense of shared responsibility and accountability. Come away with actionable steps to spearhead the development of a robust culture of cybersecurity within your organization.

HEALTHCARE INNOVATION: A SAFE AND SECURE APPROACH

Jason Wessel, Principal Solutions Consultant, Palo Alto Networks
Donny Wilson, Principal Solutions Architect, Amazon Web Services

Digital innovation continues to improve patient outcomes and accelerate accessibility and equity of care while new digital technologies are empowering patients to engage in their care from anywhere. This profound transformation has enhanced the efficiency and productivity of healthcare professionals to make informed data-driven decisions, coordinate care more effectively, and ensure the continuity of care across multiple medical disciplines. Advanced analytics and AI tools help healthcare providers derive insights from vast amounts of valuable healthcare data. This enables evidence-based decision-making, personalized treatment plans, predictive analytics for population health management, and contributions to clinical research and innovations.

PANEL: ARTIFICIAL INTELLIGENCE: CYBERSECURITY'S FRIEND OR FOE?

Barbee Mooneyhan, Vice President of Security, IT, and Privacy, Woebot Health
Benoit Desjardins, Professor of Radiology and Medicine, UPENN Medical Center
Eric Liederman, Director of Medical Informatics, Kaiser Permanente
Brian Anderson, Chief Digital Health Physician, MITRE

Artificial Intelligence (AI) continues to propel cybersecurity into an unprecedented era, as it simultaneously offers benefits and drawbacks by assisting both aggressors and protectors. Cybercriminals are harnessing AI to launch more sophisticated and novel attacks at large scale. And cybersecurity teams are using the same technology to safeguard their systems and data. This panel unpacks the implications of both offensive and defensive AI and examines new risks introduced by ChatGPT and other types of generative AI. You'll come away with actionable guidance to mitigate the increased risks associated with AI and stay secure in an unpredictable threat landscape.

CYBER, AI, AND IP REGULATORY UPDATES

Lee Kim, Senior Principal, Cybersecurity & Privacy, HIMSS

Get an overview of the latest updates in laws and regulations relating to cybersecurity, artificial intelligence, and intellectual property. You will gain an understanding of the changes to laws and regulations based upon new and emerging technology and particularly in the AI space and the threats and opportunities afforded by AI.

HOW A PHYSICIAN-OWNED PRACTICE RECOVERED FROM AN ADVANCED RYUK RANSOMWARE STRIKE

Terri Ripley, Chief Information Officer, OrthoVirginia

Two years ago, Virginia's largest provider of orthopedic medicine and therapy, OrthoVirginia, was hit with a ransomware attack that disabled access to workstations, imaging systems, backed-up data, and more. In this session, OrthoVirginia's Chief Information Officer shares a firsthand account of the cyberattack, from the critical first steps taken upon realization of the incident to their 18-month remediation process. Understand the impact ransomware had on the practice and the non-traditional steps taken to maintain patient care. Come away with lessons learned from OrthoVirginia's experience and the steps they've taken to fortify attack surfaces from future incidents, including a more comprehensive cyber hygiene strategy.

PANEL: HOW THE U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES IS DRIVING ACCOUNTABILITY AND COMPETENCY IN CYBERSECURITY

Thomas Christl, Branch Chief, Infrastructure Analysis and Partnerships Branch, HHS ASPR
Nicholas Heesters, Senior Advisor for Cybersecurity, U.S. Department of Health and Human Services, Office for Civil Rights (OCR)
Nick Rodriguez, HHS 405(d) Program Manager, U.S. Department of Health and Human Services
Erik Decker, Vice President & Chief Information Security Officer, Intermountain Health

This panel convenes government officials from various HHS agencies to discuss their latest initiatives aimed at strengthening the HPH sector's cybersecurity posture to further enforce patient safety. Get an overview of available resources, products, and tools that help raise awareness and provide vetted cybersecurity practices. Unpack regulatory updates impacting the healthcare industry, from 405(d) and the latest HICP 2023 Publication to HIPAA and the potential impact of privacy rule changes. Come away with insights into public-private partnerships, including government and industry stakeholders supporting the HPH sector.

HIMSS

HEALTHCARE CYBERSECURITY FORUM

7-8 September, 2023 | **Boston**

AGENDA *(SUBJECT TO CHANGE)*

WORKSHOP: MOVE FASTER, SMARTER AND MORE SECURELY: BUSINESS ENABLEMENT THROUGH SECURITY

Barbee Mooneyhan, Vice President of Security, IT, and Privacy, Woebot Health
Jules Ellis, Vice President of Finance, Woebot Health
Janice Reese, Advisory Member, HSCC Cybersecurity Working Group & BISO Affiliate Leader, WiCyS

Threats are becoming more mature. Regulations are expanding and changing rapidly. Our technology is more complex, with AI becoming mainstream and the rapid migration to the cloud. This ever-changing landscape of security and privacy requires a shift in the way we bring security to business conversations. Security exists to help protect the business and those that are in their purview by helping them make sound risk-based decisions to ensure the health, success, and longevity of an organization.

During this interactive exercise, you'll will be divided into teams representing various roles within an organization and tasked with navigating through a security business challenge. Unpack the organizational-wide impact of a security incident as you assess the risk from each business lens, come up with a solution, figure out how to implement the solution, and track effectiveness. Come away equipped with the knowledge to advocate security as a business enabler instead of an antiquated cost or service lane approach.

CYBER RESILIENCY IN A HYBRID MULTI-CLOUD WORLD

Rick Bryant, Healthcare Chief Technology Officer, Veritas

Healthcare rapidly adopted the cloud to become agile during the pandemic and to provide necessary technology when the supply chain could not. Although this was a major advancement for health systems, it did not come without new and serious challenges. PHI can now be found in multiple data centers and in multiple clouds. Bad actors continue to specifically target healthcare and both the cloud and business associates remain a key entry points. Please join Veritas to learn how to become cyber resilient AND cost-effective in the new world of the hybrid, multi-cloud.

PANEL: IOT, IOMT, AND OT: SAFEGUARDING THE CONNECTED HOSPITAL

Benoit Desjardins, Professor, University of Pennsylvania Medical Center
Ali Youssef, Director, Medical Device and IOT Security, Henry Ford Health
John Vecchi, Chief Marketing Officer, Phosphorus

Medical device security is arguably one of the biggest security challenges healthcare organizations face today. And as more network-connected devices are developed and integrated into hospital workflows, cybersecurity is becoming more of a priority than ever before. In this panel, cybersecurity experts will discuss the current state of medical device security, key regulatory guidelines, and the importance of collaboration across the supply chain and beyond, from regulators to manufacturers and providers. Come away with actionable steps to combat escalating medical device security concerns, including expert recommendations for navigating new and forthcoming IoMT regulations.

MITIGATING RISKS IN HEALTHCARE AT HOME SETTINGS

Kevin Littlefield, Principal, Cybersecurity, MITRE

A remote and mobile world is upon us, and we rely on technology to help us with our lives, including how people manage their health. One burgeoning area that has seen growth is the concept of "healthcare at home" where patients engage with care teams using technology to capture health data and to interact with health information systems. We'll discuss how hospitals may apply risk management approaches to assure safeguarding on patient data using a smart home integrated setting.

PERSONAL SAFETY: HOW CYBERSECURITY AND PRIVACY PROTECTION GENERATE TRUST IN THE HEALTHCARE SYSTEM

Eric Liederman, Director of Medical Informatics, Kaiser Permanente

The effective protection of PHI is essential to maintain the confidence and trust of physicians, healthcare employees, and most importantly—patients—in the healthcare system. And if patients don't trust their health systems to protect their privacy and data, then they won't use their services. Get best practices to promote a sense of trust by prioritizing PHI security and upholding the ethical and legal obligations associated with handling sensitive medical information.

PANEL: REVAMPING YOUR CYBERSECURITY STRATEGY FOR 2023 AND BEYOND

Andrea Fox, Senior Editor, Healthcare IT News, HIMSS
Terri Ripley, Chief Information Officer, OrthoVirginia
Margie Zuk, Senior Principal Cybersecurity Engineer, MITRE
Jonathan Shannon, Associate Vice President of Healthcare Strategy, LexisNexis Risk Solutions

Today's interconnected and digitized world —coupled with more sophisticated cyber attacks— exposes new vulnerabilities and requires organizations to reevaluate their cybersecurity posture. Get updated recommendations from MITRE around medical device security, incident preparedness and response, and more—and how to factor them into your overall cybersecurity strategy. Come away with actionable guidance for refining your cyber roadmap to ensure resilience in an evolving landscape, tackle future challenges, and proactively respond to emerging threats.

CLOSING KEYNOTE: A COLLABORATIVE APPROACH TO MITIGATING CYBERCRIME IN HEALTHCARE

William Scott O'Donnell, Supervisory Special Agent, FBI
Joelle Calcavecchia, Staff Operations Specialist, FBI

Join FBI special agents William Scott O'Donnell and Joelle Calcavecchia as they addresses the rise in cybercrime against health systems and how the FBI can help –whether it's to prevent a suspected attack or respond to a ransomware incident. Drawing from real-world examples and decades of field experience, they will clear up common misconceptions about incident response and walk through what happens when healthcare organizations reach out for help. Discuss the importance of collaboration and get tips for incident reporting, threat intelligence, information sharing, and more.