CYBER WORKSHOP
JUNE 14, 2022
AGENDA

9:00 am – 9:30 am	**Continental Breakfast and Registration**
9:30 am - 10:30 am	**Overview of Cyber Threat Landscape Panel – the FBI and the AHA:** (1 hour) ***(Joint presentation with John Riggi and local FBI representative)*** • Learn from the FBI cyber program leaders about the criminal and national security cyber threats they are investigating on a global, national, and regional level. • Learn how best to work with the FBI and other government agencies, prior, during and post cyber incident. • The FBI will also discuss and distinguish their non-regulatory role in the investigation of cyber incidents and how they work with DHS, CISA, HHS and other national security agencies. • Learn what hospitals and healthcare systems on a national level are saying to their trusted AHA cyber advisor about their biggest cybersecurity threats challenges. • Learn how the AHA is helping the field mitigate those threats and exchange information with the FBI and other government agencies.
10:30 am - 10:45 am	**Break / Visit Exhibitor**
10:45am - 11:25 am	**Lessons Learned and Best Practices from Cyber Attack Victims** (40 min) ***(Moderated panel discussion with John Riggi which may include cyber-attack victim)*** • One guest speaker (CEO, CIO or CISO) from Puerto Rico's large hospital/health system • One guest speaker (CEO, IT or Security Director or equivalent) from Puerto Rico's small/rural hospital
11:25 am - 12:05 pm	**Cyber Risk as Enterprise Risk + Ransomware Preparedness and Response** (40 min) ***(Moderated Presentation and discussion with attendees and previous panelists)*** • Cyber survey results will be discussed. • AHA John Riggi will present national perspective on ransomware attacks based upon direct interaction and discussion with victim organization and government agencies. • Also discuss how cyber risk translates into enterprise risk issues with direct implications to revenue, reputation, care delivery and patient safety. • Learn how your organization may be carrying hidden strategic cyber risk through third party relationships. • Discuss cyber enterprise risk communication and risk mitigation strategies with your non-technical peers and leadership. • Exchange ideas to assist in creating an organizational culture of cybersecurity and facilitate cyber resource requests between technical and non-technical leadership.
12:05 pm - 1:00 pm	**Lunch** Networking and open discussion

PM Agenda

1:00 pm - 2:30 pm	**Cyber Table-top Exercise** John Riggi will moderate and actively engage all attendees in a group critical thinking and strategic leadership cyber incident exercise. The session is designed to be highly interactive and isbased upon real world complex and multi-faceted cyber and risk incidents. It is designed for both technical and non-technical leaders and structured to test incident response plans, identify gaps, and elicit strategic decision-making skills under simulated adversarial conditions. John will directly solicit responses from the audience at all key decision points.
2:30 pm - 3:00 pm	**Wrap-up, lessons learned and discussion.** ***What changes will you and your organization make to improve cybersecurity as result of what you have learned in this workshop?***

John Riggi - National Advisor for Cybersecurity and Risk

AHA Cybersecurity & Risk Advisory

jriggi@aha.org

+1 202-626-2272

John Riggi, having spent nearly 30 years as a highly decorated veteran of the FBI, serves as the first senior advisor for cybersecurity and risk for the American Hospital Association and their 5000+ member hospitals. John leverages his distinct cyber, criminal investigation and national security experience at the FBI and CIA to provide trusted strategic cyber and risk advisory services to the nations' hospitals and health systems.

His trusted access to healthcare leaders and government agencies enhances John's unique national perspective on cyber and risk issues and greatly contributes to the AHA's policy and advocacy efforts. John represented the nation's hospitals in testimony before the Senate Homeland Security Committee hearing on cyber threats to hospitals in Dec. 2020. This assisted in the passage of PL 116-321, providing regulatory relief for HIPAA covered victims of cyber attacks. In 2021, John's prominent advocacy encouraged the government to raise the investigative priority level of ransomware attacks to equal that of terrorist attacks.

In various leadership roles at the FBI, John served as a representative to the White House Cyber Response Group and a senior representative to the CIA. He also served as the national operations manager for terrorist financing investigations. John also led counterintelligence field surveillance programs in Washington DC and financial crimes and terrorist financing squads in New York City. John ultimately rose to the ranks of the Senior Executive Service and in that capacity led the FBI Cyber Division national program to develop mission critical partnerships with the healthcare and other critical infrastructure sectors. John held a national strategic role in the investigation of the largest cyber-attacks targeting healthcare and other sectors.

He also served on the NY FBI SWAT Team for eight years. John is the recipient of the FBI Director's Award for Special Achievement in Counterterrorism and the CIA's George H.W. Bush Award for Excellence in Counterterrorism, the CIAs highest award in this category. John presents extensively on cybersecurity and risk topics and is frequently interviewed by the media.

GMsectec