PROTECT YOUR ORGANIZATION'S RESILIENCY WITH AHA'S CLINICAL CONTINUITY ASSESSMENT PROGRAM

How Would You Provide Care for 30 Days Without Technology?

With cyberattacks against hospitals and mission-critical third-party providers escalating in both frequency and severity, it's an unfortunate reality that continued attacks are inevitable. Not only do these incidents represent data theft and financial crimes, but for hospitals, they are threat-to-life crimes designed to shut down vital systems and cause maximum delay and disruption to patient care.

How prepared is your hospital to continue providing life-saving care during an extended disruption? Given the prevalence of attacks and the disruption caused by ransomware, ensuring that your hospital can continue to provide safe and quality care without critical technology for at least 30 days is not just an option: It's a necessity.

The **AHA Clinical Continuity Assessment Program** helps you evaluate your hospital's readiness to maintain patient care during such disruptions. Led by our team of nationally recognized and uniquely experienced health care cybersecurity experts, this comprehensive assessment provides the insights, recommendations and structure needed to ensure your organization can function without access to mission-critical and life-critical technology.

What We Do

Our trusted experts help you understand, how well your hospital is prepared to maintain critical clinical and operational functions during a cyberattack. Our Clinical Continuity Assessment Program goes far beyond traditional cybersecurity checks; we dig deep into plans, conduct interviews and visit care sites. Leveraging our experience in assisting hundreds of ransomware victims, we provide specific strategic and operational recommendations across all functions — to maintain clinical continuity and business resiliency during prolonged outages.

> "The question isn't if an attack will happen. The question is: are you ready?"
>
> – **John Riggi**
> National Advisor for Cybersecurity and Risk for the **American Hospital Association** (AHA)

Why It's Critical

- **Cyberattacks Are Inevitable:** Hospitals are prime targets for ransomware attacks that threaten not just data, but life-saving care. It's not a matter of "if," but "when."
- **Regulatory Review:** Hospitals should have disaster recovery, continuity and emergency management plans to meet key recommendations, including for cyber incidents.
- **Protect Your Reputation & Patients:** Disruptions in clinical care can damage your hospital's reputation and erode patient trust.

How We Help

Our methodology, developed by AHA's experts, is a hands-on, thorough review of your readiness, response and resiliency capabilities. The process is based upon the experiences of hundreds of leaders who experienced ransomware attacks at other organizations and the results of over 100 ransomware cyber tabletop exercises. It includes:

- **Interviews with key leaders** to understand your current capabilities and needs.
- **In-depth document reviews** to evaluate your existing plans.
- **Team discussions** to align strategies across departments.
- **On-site visits** to inform insights and deliver actionable recommendations.

What We Evaluate

We'll dive deep into your hospital's preparedness, focusing on the following critical areas:

- **Cybersecurity & Resiliency:** Is your IT infrastructure equipped to respond to cyberattacks and continue operations without systems for at least a few weeks?
- **Clinical Continuity:** Can your clinicians maintain high-quality patient care without access to EHR/EMR systems or other key technologies?
- **Disaster Recovery:** How quickly can your hospital recover, and what's your downtime plan for maintaining operations during an extended event?
- **Third-Party Dependencies:** Are your external service providers prepared to handle disruptions to ensure continuity of care?

What You'll Gain

Our Clinical Continuity Assessment Program doesn't just provide you with a list of findings — it gives you **actionable insights** and **practical recommendations** to strengthen your hospital's ability to respond to a cyberattack:

- **Real-World Readiness:** Prepare to maintain care, even without access to critical systems.
- **Robust Response Plans:** Ensure every staff member knows their role in a crisis.
- **Improved Recovery Times:** Minimize downtime and accelerate your recovery efforts.
- **Meet Key Recommendations:** Meet industry best practices and other key recommendations seamlessly.

Why AHA?

As the nation's leading advocate for hospitals, the AHA is uniquely positioned to help you navigate the complexities of cybersecurity and physical security in health care. Our team of cyber and physical security experts combines real-world health care experience to help you face the evolving landscape of cyberthreats, so you can safeguard your clinical operations and ensure patient safety.

About John Riggi

John Riggi, national advisor for cybersecurity and risk at the American Hospital Association, brings nearly 30 years of distinguished service with the FBI, specializing in cyberthreats, organized crime and terrorism. At the AHA, he leverages his expertise to provide risk advisory services, assist ransomware victim hospitals, and lead initiatives like the joint HHS hospital cyber resiliency report and voluntary cybersecurity performance goals. A trusted advocate, John has testified before Congress, influenced key cybersecurity legislation, and collaborated with government agencies to enhance hospital defenses. A former senior executive service member at the FBI, he managed critical partnerships across infrastructure sectors and played a strategic role in investigating major cyberattacks. John's extensive field experience, including SWAT and counterintelligence operations, has earned him accolades like the FBI Director's Award and the CIA's George H.W. Bush Award. He is a sought-after speaker and media expert on cybersecurity.

About Scott Gee

Scott Gee, a seasoned cybersecurity leader, is the deputy national advisor for Cybersecurity and Risk at the American Hospital Association, with extensive experience in both public and private sectors. Before joining the AHA, he served at Microsoft, safeguarding critical networks and assets as a senior cyber incident response manager. Scott's 22-year career with the U.S. Secret Service (USSS) included groundbreaking roles, such as leading the Counter Drone Unit and Airspace Security Branch, founding the UK Electronic Crimes Task Force, and setting standards in digital forensics. He also provided protective services for U.S. leaders and helped shape initial policies for the Cybersecurity and Infrastructure Security Agency. A certified information systems security professional, Scott is a recipient of the USSS Director's Award and a sought-after speaker on cyber defense topics.

Cyberthreats Won't Wait, and Neither Should You.

Contact Us to Learn More and Schedule Your Assessment Today!

American Hospital Association | 155 N. Wacker Drive, Suite 400 | Chicago, IL 60606

For more information, please contact Karen Sethney at **ksethney@aha.org** or call **(312) 422-2075**