MEDTECH SEMINAR

WEDNESDAY, OCTOBER 30
9:15 AM – 3:30 PM
Minneapolis Marriott Northwest

Minnesota became 'medical alley' for having the world's largest concentration of medical device companies. Notwithstanding mergers and acquisitions, this remains the heartbeat of healthcare, and the "do no harm" duty of care requires an embedded expectation of solid cyber security – for data and devices.

9:15 AM — MedTech Seminar Welcome
Start the day with a history of the Cyber Security Summit critical infrastructure seminars. The MedTech marks the eighth year here for healthcare conversations across public and private interests. A quick review of today's agenda and group goals will get us to "go"!

9:30 AM — Fighting the Dragon: IoT for Medical Devices
As medical capital equipment and programmers increasingly connect to the internet for updates, so too increases the pressure to keep the management system up to date. Review and examine security best practices for the Med Dev Internet of Things.

10:00 AM — They Did What? Learning from Others' Med Device Cybersecurity Mistakes
Since March of 2023, cyber device manufacturers have been required to submit information that demonstrates effective device protection from cybersecurity threats. We'll discuss what's required for PMA, PDP, HDE and the other submission types, and learn from FDA feedback provided to companies during the first year of corporate compliance.

10:50 AM — Musings From My Forever Spent in Medical Device Cybersecurity
Ken Ya HoyMe now? It's 2024, devices are secure, with high customer confidence ratings. But twenty years ago, few thought about security, and those who raised flags battled "who would want to do that?" pushback. Hear the war stories and key battles that led to today's tremendous cross-stakeholder collaboration and core investment in cybersecurity.

11:20 AM — MT 5 - Navigating Transparency - Sharing Cybersecurity Information with HDOs
Cyber attacks are a high-volume, regular occurrence, creating the need for device manufacturers to share product vulnerability information with healthcare delivery organizations - to protect their systems and facilities against potential threats. Abbott shares information with HDOs today in a centralized manner: learn about the journey to get this robust program in place.

12:45 PM — Navigating the Complexities of Biomedical Device Vulnerability Management
From wearable health monitors to complex diagnostic machines, traditional security measures often fall short, leaving patient safety and data at risk. This panel will get specific on the legacy systems, proprietary protocols and 'no downtime' challenges that make biomedical devices notoriously difficult to scan and secure.

1:30 PM — Preparing the Next Generation of Cybersecurity Professionals for the Real World
Metropolitan State University has developed an elite academic cybersecurity program with undergraduate and graduate degrees and hands-on experience through organizational partnerships that prepare students for meaningful jobs. Hear about the program's depth and breadth with a comparative analysis to similar programs

2:30 PM — Threat Model: Prevent Security Incidents (the right way)
Learn to build robust threat assessments that pinpoint essential security controls early in the medical device development design phase. We'll take top challenges and share specific strategies to keep threat models manageable, approachable, and defendable – from beginning to end.

3:00 PM — Leveraging JSP2 to Mature Healthcare Product Security Programs
Cybersecurity is everyone's responsibility, so the Healthcare and Public Health Sector Coordinating Council has drafted a Joint Security Plan, a secure product development framework used to develop, deploy, and support cybersecure technology solutions in healthcare environments. Learn about this voluntary program and its value to organizations large and small.

MedTech Supporter

asimily

Register at cybersecuritysummit.org
$299 registration fee includes lunch.

24-10-14