MEDICAL DEVICE CYBERSECURITY WORKSHOP

PATIENT SAFETY • CRITICAL INFRASTRUCTURE • POPULATION SAFETY
DEVICE MANAGEMENT • BEST PRACTICES • REGULATORY COMPLIANCE
RISK MANAGEMENT • THREAT INTELLIGENCE • VULNERABILITY MANAGEMENT

JUNE 12, 2017
We’re so glad you’re able to join us in Tampere for what promises to be a great event. On the following pages, you’ll see an exciting agenda that includes 3 major sessions of 90 minutes each. Each one of these major sessions is composed of two sessions; each of these sessions will be 45 minutes. The first is the ‘Foundations’ session and it will cover the key concepts from a technical, science, or policy perspective. The second session presents real-world experience that will reinforce the concepts from session one and will assist attendees in applying the learning from these sessions. You’ll also see the biographies of many of the presenters and panelists that will be part of the workshop. The following provides a general overview of the workshop hosts: EMBEC, MDISS, and NH-ISAC.

**Medical Device Innovation, Safety and Security Consortium (MDISS)** is a collaborative and inclusive non-profit professional organization committed to advancing quality health care with a focus on the safety and security of medical devices. MDISS builds solutions through collaboration with providers, payers, manufacturers, universities, government agencies, technology companies, individuals, patients, patient advocates, and associations to reduce risk in the U.S. biomedical device network. MDISS is focused on optimizing the relationship between the quality of health care and the safe process of assessing and ensuring that devices and systems are secure and functioning in a safe and efficacious manner.

**National Health Information Sharing and Analysis Center (NH-ISAC)** is the official healthcare information sharing and analysis center, offering non-profit and for-profit healthcare stakeholders a community and forum for sharing cyber and physical security threat indicators, best practices and mitigation strategies. Membership is open to any healthcare stakeholder seeking protection of valuable PHI (personal health information) and IP (Healthcare-related Intellectual Property) and also compliance with Federal HITECH ACT, HIPAA-related privacy rights and NIST (National Institute of Standards and Technology) guidelines. NH-ISAC is a non-profit corporation funded, owned and governed by its members. Members include private & public hospitals, “ambulatory” providers, health insurance “payers,” pharmaceutical/biotech manufacturers, laboratory, diagnostic, medical device manufacturers, medical schools and medical R&D organizations. Joining NH-ISAC is one of the best ways health care and public health firms can actively participate to protect the industry and its vital role in critical infrastructure.

**EMBEC 17** is the joint conference of the European Medical and Biological Engineering Conference (EMBEC) and the Nordic-Baltic Conference on Biomedical Engineering and Medical Physics (NBC), in Tampere, Finland, in June 2017. These two long running conferences are now combined for the first time with aim to build a truly cross-discipline conference. We aim to present all traditional BMES and BME areas, but also highlight new emerging fields, such as tissue engineering, bioinformatics, biosensing, neurotechnology, additive manufacturing technologies for medicine and biology, and biimaging, to name a few. Moreover, we will emphasize the role of education, translational research, and commercialization.
MEDICAL DEVICE CYBERSECURITY WORKSHOP – June 12, 2017

AGENDA

10:45 – 12:15  Core Concepts: Medical Device Cyber Security
   a. Foundations (60 min)
      • Background, growing interest
      • Multiple cyber risk domains
      • The security risk function
      • Remediating risks through controls
   b. Experience (30 min)
      • Establishing a medical device security program
      • Stakeholders in the ecosystem
      • Collaboration to reduce risk

12:15 – 13:15  Lunch

13:15 – 14:45  Medical Device Post-Market Risk Management
   a. Vulnerability Management (30 min)
      • Medical device 'vulnerability': Challenges in definition and identification
      • Vulnerability scoring methods: Strengths and weaknesses
      • Vulnerability tracking methods
   b. Threat Intelligence (30 min)
      • Medical device cyber surveillance defined and understanding its importance
      • Understanding threat intelligence for medical devices
      • Relationship between threat intelligence and risk assessments for medical devices
      • Updates on the National Cyber Safety Network: An analog to the National Health Safety Network (NHSN) in the USA
   c. Information Sharing to Reduce Risk (30 min)
      • Lessons from 7 years of public-private-partnership collaborations in the USA
      • Challenges in the sharing of vulnerabilities: what, when, where and how?
      • Medical Device Intelligence Program for Evaluation and Response (MD-VIPER): A private sector operated vulnerability reporting service for manufacturers
      • Experiences with initiatives to improve medical device threat intelligence
      • Reflections on how little is known about medical device cyber risk, associated human exposure, and its relationship to patient safety
14:45 – 15:45 Networking Break

15:45 – 17:15 Medical Device Risk Management and Assessment Methods (90 min)
  a. Foundations (45 min)
    - Understanding risk management and risk assessment across the life cycle
    - Executing risk assessment: Defining the process and its challenges
    - International standards for medical device risk: Explanation and update
    - Understanding the importance of medical device risk assessments
  b. Experience (45 min)
    - Experience using a cloud-platform for risk assessments: Crowdsourcing for the conservation of resources, improving assessment accuracy, and improving the assessment methodology
    - Executing an enterprise-wide risk assessment program for medical devices: Planning and executing experience
    - Medical device workforce challenges, impact on risk assessment programs, and on patient safety
    - Timelines to more secure devices: From requirements to procurement
DENISE ANDERSON, MBA
President, National Health Information Sharing and Analysis Center (NH-ISAC)

Denise Anderson is the President of NH-ISAC and currently serves as Chair of the National Council of ISACs and participates in a number of industry groups such as the Cross-Sector Cyber Security Working Group (CSCSWG). She was instrumental in implementing a CI/KR industry initiative to establish a private sector liaison seat at the National Infrastructure Coordinating Center (NICC), CI/KR community and the federal government and serves as one of the liaisons. She is a financial and health sector representative to the National Cybersecurity and Communications Integration Center (NCCIC) and sits on the Cyber Unified Coordination Group, (UCG).

Denise is certified as an EMT (B), Firefighter I/II and Instructor I/II in the state of Virginia, and is an Adjunct Instructor at the Fire and Rescue Academy in Fairfax County, Virginia. She is also certified under the National Incident Management System (NIMS). In addition, she has served on the Board and as Officer and President of an international credit association. Denise holds a BA in English, magna cum laude, from Loyola Marymount University and MBA in International Business from American University. She is a graduate of the Executive Leaders Program at the Naval Postgraduate School Center for Homeland Defense and Security.

DALE NORDENBERG, MD
Co-founder and Executive Director, Medical Device Innovation, Safety, and Security Consortium (MDISS)

Dr. Nordenberg is the co-founder and Executive Director for the Medical Device Innovation, Safety, and Security Consortium (MDISS). He is a member of the Health Information Technology Standards Federal Advisory Committee (ONC, HHS); a member of the FDA's National Evaluation System for Technology (NEST) Planning Board; and co-chairs the Medical Device Security Information Sharing Council for the National Health Information Sharing and Analysis Center (NH-ISAC). Dr. Nordenberg is CEO of Novasano Health and Science. He has extensive experience in the domains of healthcare strategy and operations, health information technology, FDA regulated industries, research network development, public-private partnership development, and emergency preparedness.

Dr. Nordenberg also cofounded and co-directs the public-private partnership, TBResist. Prior to Novasano, Dr. Nordenberg was a managing director in the health care practice of PricewaterhouseCoopers. Dr. Nordenberg held various positions at CDC including Chief Information Officer (CIO) and Associate Director, National Center for Infectious Diseases (NCID). He was detailed to the Office of the National Coordinator for Health Information Technology at HHS. Dr. Nordenberg was a member of the Science and Technology Review Subcommittee of the Science Advisory Board of the FDA. Prior to CDC, Dr. Nordenberg was a founding executive of a company that launched VeriSign affiliates in Latin America and Asia and prior to that he was faculty in the Emory School of Medicine where he founded and directed the Office of Medical Informatics for the Emory University Children’s Center and was the physician lead at Egleston Children’s Hospital.

Dr. Nordenberg is a board certified pediatrician, medical epidemiologist, and medical informaticist. He received a BS in Microbiology from the University of Michigan, his medical degree from Northwestern University, completed his training in pediatrics at McGill University, Montreal Children’s Hospital, and his fellowship in epidemiology and public health in the Epidemic Intelligence Services Program at the Centers for Disease Control with a focus on “big data”.
ABOUT THE EXPERTS

MICHAEL McNEIL, MBA
Global Product Security & Services Officer at Philips Healthcare

Leader with extensive years of business experience known for getting the job done and making the tough decisions while enabling those that work with and for him to grow and reach their potential.

A Global Chief Security & Privacy Officer whose performance excellence, an unrelenting results focus and aggressive implementation with an indelible commitment to ethical business practices and superior services has lead key transformational areas in Product, IT, Privacy and Physical Security space for organizations like Philips, Medtronic, Liberty Mutual, Pitney Bowes, Reynolds & Reynolds, Johnson & Johnson and AT&T over his career.

Specialties: Growing profits; turning around businesses; leading people, mentoring, marketing, product management & development experience; telecommunication industry experience, healthcare industry experience, automotive industry experience, IT, global privacy & data security experience, PCI credit card compliance; and strategy development to name a few areas.

AAPO CEDERBERG
Executive Adviser, Associate Fellow at the GCSP, Colonel (G.S. Ret.)

Aapo Cederberg’s current position is Executive Adviser to the Finnish Information Security Cluster (FISC). He is also an Associate Fellow of the Global Fellowship Initiative at the Geneva Centre of Security Policy (GCSP). His main area of responsibility is Cyber security and other comprehensive security matters such as Hybrid warfare and to organize training courses and security dialogue on this topic.

Mr. Cederberg has served as a Secretary General for the Security Committee of Finland for six years. The Security Committee provides support, advice and expertise for the government in comprehensive security matters and serves as a collaborative platform for the on-going national efforts related to the national crisis preparedness. Mr. Cederberg’s earlier assignments include working as the head of Strategic Planning and foresight at the Ministry of Defence (2005 – 2007). Before this he has a long career in the service of Finnish Armed Forces, where his latest assignments include holding the Commander position at the Häme GBAD Battalion (2003 – 05) and serving as a Senior Military Adviser at the Permanent Mission of Finland to the OSCE (1999- 2003).

ERIKA SUORTTI-MYYRY

Erika Suortti-Myyry has worked for the Finnish National Cybersecurity Centre and its predecessor CERT-FI since 2007. Her current responsibilities include ICS security, health sector cooperation and systems development. Previously, she has worked as a duty officer and as a situation coordinator for the NCSC-FI situation centre.
STEVE ABRAHAMSON, MBA
Senior Director of Product Security, GE Healthcare

Steve Abrahamson is Senior Director of Product Security at GE Healthcare, based in his hometown of Waukesha, Wisconsin. Steve’s leads the GE Healthcare Product Cyber Security organization in development and implementation of the GE Healthcare Design Engineering Privacy and Security process across all global product lines, as well as development of security systems and tools, integration of security within strategic software programs, and development of collaborative approaches with customers, regulators, and industry groups.


Steve is a certified Six Sigma Black Belt and Master Black Belt, and has a Bachelor’s Degree in Mechanical Engineering from Marquette University and a MBA from the University of Dallas. Steve also represents GE as a member of GE’s corporate marathon team, and he has completed over 120 marathons.

JARI SEPPALA
Project Manager, TUT Automation and Hydraulic Engineering

Jari Seppälä, M.Sc., holds 18 years of expertise in securing critical infrastructure via hands-on industrial projects, research and education. For Jari, information security is a risk management tool which enables dependable critical infrastructure whether automation in power production, everyday goods or medical environments. Jari’s background in data analysis and control systems theory provides him a solid domain understanding and ability to implement security without compromising the functionality of the time critical systems.

Martti Lehto

Martti Lehto, PhD (Military Sciences), Col (ret.) is Professor in Cybersecurity in the University of Jyväskylä in the Faculty of Information Technology. He has over 30 years’ experience as developer and leader of C4ISR Systems in Finnish Defence Forces. Now he is a Cyber security and Cyber defence researcher and teacher and the pedagogical leader of the Cyber Security MSc. program. He is also Adjunct professor in National Defence University in Air and Cyber Warfare. He has about 100 publications, research reports and articles on areas of C4ISR systems, digitalization, cyber security and defence, information warfare and defence policy. Since 2001 he has been the Editor-in-Chief of the Military Magazine.
ABOUT THE EXPERTS

Justin Cappos

Justin Cappos is a tenure-track assistant professor in the Computer Science and Engineering department at New York University. Justin's research philosophy focuses on improving real world systems, often by addressing issues that arise in practical deployments.

His security systems for securing software updates are adopted into a wide array of software, including automobiles, popular cloud technologies, and most Linux systems. His research advances are used in production use in a variety of other widely used software including git, Python, and Docker. Due to the practical impact of his research, Justin has received several awards including being named to Popular Science’s Brilliant 10 list in 2013. More information is available at https://ssl.engineering.nyu.edu/personalpages/jcappos/

Jari Knuuttila, Senior Officer. National Supervisory Authority for Welfare and Health (Valvira).

Supervising medical devices and their safe use in Finland. Market surveillance and vigilance issues, mainly focused on electrotechnical medical devices. Medical device software conformity assessment.

Phillip M. Englert
National Director Technology Operations – Physical Asset Services

A recognized thought leader responsible for developing and delivering support initiatives for healthcare technology. Phil leads medical device cybersecurity initiatives, a medical device self-insurance extended warranty program, and the business resilience team for Catholic Health Initiatives. Operationalized medical device security risk assessment and a multi-disciplinary standard configuration team to reduce vulnerability footprint on clinical equipment. Has actively collaborated with DHS, FDA, NH-ISAC, and several manufacturers and healthcare providers to advance cyber information sharing in the healthcare community. Phil leads collaborative efforts with emergency management and information technology infrastructure leaders to support business continuity planning at CHI care delivery facilities and supporting services. Phil’s specific areas of interest include comprehensive benchmarking of healthcare technology maintenance activities for over 100 acute care centers to optimize and amplify business unit strengths through data driven decision support.

Phil, a Thomas More College graduate, has worked for Catholic Health Initiatives since 1994 and has over 31 years of experience in technical service and management of healthcare and scientific technologies. Phil expanded his skills and expertise through affiliations with COHR Masterplan, Labtronics, Inc., Fisher Scientific, Instrumentation Laboratories, Langham-Mathis Instruments, and the United States Air Force.