Advancing Healthcare Cybersecurity Knowledge

September 10, 11 and 12, 2018
University of Delaware

John M. Clayton Hall, Newark, Del.
Conference sponsored by UD's Cybersecurity Initiative and College of Health Sciences

www.pcs.udel.edu/health-cybersecurity

CONFERENCE SCHEDULE

Monday, September 10, 2018

1:00 to 4:30 p.m.

12:30 to 1:00 p.m.—Registration with Light Breakfast

1:00 to 2:00 p.m.—Cybersecurity: The Role of the Healthcare Provider and Agency Caring for the Whole Person Including Personal Health Information—Mike Maksymow, MBA/TM, CHCIO, FCHIME, FHIMSS, CPHIMS, Vice President & Chief Information Officer, Beebe Health, Lewes, Delaware

The goals of any healthcare provider and agency are to provide safe, cost-effective, quality care. Today, this care must also include protection of the patient's private health information to support the patient/provider relation and build trust. Mr. Maksymow will share his vast experience as Beebe Health's top protector of patient information looking at the world of cybersecurity through the lens of those who deliver care. His talk will share defensive strategies in which the audience can immediately apply to improve their organization's security posture and allow patients to rely on the integrity and strength of the healthcare entity.

2:00 to 2:30—Break with Snack

2:30- 3:30 p.m.—Cybersecurity Implications of Blockchain in Healthcare—Heather Flannery, Health Circle Global Lead, ConsenSys; Co-Founder & Board Chair, BiHG, IEEE ISTO; Co-Chair, HIMSS Blockchain Task Force

Blockchain is hailed by many in the patient data management field as a way to securely track information moving between patients and healthcare providers and payers, giving patients stewardship over their health information. Ms. Flannery, an entrepreneurial leader in the field of

Blockchain technology, will introduce the audience to current opportunities in blockchain and distributed ledger technologies. Listeners will gain insight into the values and barriers related to adoption of this technology in both national and global arenas. Ms. Flannery will discuss the relationship between blockchain and cryptoassets, and help the audience recognize the role of blockchain in the convergence of 4th Industrial Revolution technologies.

3:30 to 4:00—Networking

Tuesday, September 11, 2018

8:30 to 4:30 p.m.

8:30 to 9:00 a.m. —Registration with Light Breakfast

9:00 to 10:00 a.m.—Evolving Medical Device Cybersecurity—Julie Connolly, CISSP, Principal Cybersecurity Engineer, The MITRE Corporation

Medical devices have evolved from standalone systems to implanted devices, networked systems, and even apps that are now integrated with electronic health records, IT networks, and more. As a result, cybersecurity has not always been a medical device design consideration. For the last several years, the U.S. Food and Drug Administration (FDA) has been working to bring the community together to collectively address medical device cybersecurity. This session will review the work the FDA and others have been doing to proactively address medical device vulnerabilities and improve overall device cybersecurity, to include incorporating a Software Bill of Materials (SBOM) into premarket device requirements; streamlining the FDA pre- and post-market medical device regulatory processes into one total lifecycle approach; developing a Common Vulnerability Scoring System (CVSS) rubric to assess device vulnerability impact and severity; encouraging the emergence of Information Sharing and Analysis Organizations (ISAOs) to help broker medical device vulnerability management; and growing the use of table top and other exercises to validate vulnerability handling procedures.

10:00 to 10:15—Break

10:15 to 11:00—Defending Our Telehealth: A Threat-Based Approach—Ronnie Daldos, CISSP, MITRE Corporation

The telehealth ecosystem is a complex combination of technologies enabling new capabilities for delivery of patient centric care. This session introduces threat based defense as a key component of a comprehensive risk management strategy. A threat based approach will help identify, prioritize, and mitigate threats to secure the telehealth ecosystem.

11:00 to 12:00—Using ATT&CK to Improve Cyber Defense—Julie Connolly, CISSP, Principal Cybersecurity Engineer, The MITRE Corporation

Despite the growing use of cyber threat-based defensive techniques, breaches still occur and detecting them remains difficult. Once an attacker penetrates a network, there are numerous ways to hide

undetected. Common means to identify cyber attacker "footprints" have been elusive until now. The Adversarial Tactics, Techniques, & Common Knowledge (ATT&CKTM) knowledge base, developed for public use by the MITRE Corporation, provides a methodology for characterizing and describing the actions an adversary may take while operating on specific platforms, and prior to compromise, within an enterprise network.

12:00-1:00 p.m.—Lunch

1:00 p.m.-4:00 p.m. Best Practices for Securing Systems, People and Facilities from Cyberattacks
John Gomez is the CEO and founder of Sensato Cybersecurity Solutions

Afternoon Overview: This program will help those responsible for securing systems, people and facilities from cyberattacks to better understand the current threat landscape, as well as to better understand best practices and fallacies related to cybersecurity.

- **1:00 to 1:30 p.m.—Interpreting Threat Intelligence** – The best practices related to establishing an effective threat intelligence program, as well as the utilization of threat intelligence. The program will also look at how threat intelligence can be used to increase
- **1:30 to 2:00 p.m.—Attacker Motivation** – A high-level review of attacker motivations and psychology. This module will also provide a high-level review of current threat intelligence.
- **2:00 to 2:45 p.m.—Rational Response Theory** – RRT or Rational Response Theory, is the psychology that we apply in rationalizing threat intelligence and cybersecurity risks. During this session we will examine how RRT can impact our ability to create effective strategies and responses to potential risks and threats.
- **2:45 to 3:00 p.m.—Break**
- **3:00 to 4:00 p.m.—NIST 800-53 Dirty Dozen**—NIST 800-53 is an amazingly rich cybersecurity framework and one that is freely available. The challenge with NIST 800-53 is often the amount of resources it required to be fully implemented. Recognizing this as a problem across industries, we have developed the "NIST 800-53 Dirty Dozen." Embracing the 80/20 rule, we have identified twelve critical milestones that will take any organization from zero compliance to 80% of full adherence to NIST 800-53.

4:00 p.m.—Closing

Wednesday, September 12, 2018

8:30 to 4:30 p.m. (Workshop day)

8:30 to 9:00 a.m.— Registration and Light Breakfast

Workshop Overview: Today we will begin to delve into the psychology of the attacker, look deeper at how and why attackers are successful and begin to better understand their technical approaches by dissecting several attacks. Further, we will also look at incident response best practices and work through an incident response simulation.

Presenters: John Gomez, CEO and founder of Sensato Cybersecurity Solutions; and Brett J. Warrick, Director of Business Development at Sensato Cybersecurity Solutions

- **9:00-9:30 a.m.—Cracking the Enterprise**—A walk through an internal network compromise and how this can be used to help us better understand risk assessment strategies and approaches. We will also look deeper into the psychology and motivation of the attacker.
- **10:30 a.m.-12:00 p.m.—Dissecting Russia**—Given the threat levels that exist and are posed by Russian cyber-attackers, we will look into their TTP. By dissecting attacks against critical infrastructure and other sectors we will being to better understand how to apply defensive methods by learning from these approaches.
- **12:00-1:00 p.m. —Lunch**
- **1:00-2:00 p.m. —Advanced Attack Methods** – We will look at polymorphic attacks, malware less attacks and attacks that incorporate machine learning. This is a highly technical session that will look at the technology behind the attacks.
- **2:00-3 p.m. —Incident Response Best Practices** – We will look at the latest best practices related to incident response, such as protocols, immediate action drills and more.
- **3:00-3:15 p.m. —Break with snack**
- **3:15-4:15 p.m. —Incident Response Simulation** – We will work in small teams to walk through an actual attack and use this information to coordinate an effective and practical

4:30 —Conference End

Conference Presenters

Michael J. Maksymow, Jr., MBA/TM, CHCIO, FCHIME, FHIMSS, CPHIMS

Mike is Vice President & Chief Information Officer at Beebe Healthcare in Lewes, Delaware, and leads the Information Systems & Technology, IT Security, Project Management Office (PMO), Telecommunications, Clinical Informatics, and BioMedical Engineering teams. He has more than 20 years of progressive IT experience during which he has provided strategic direction, managed budgets and operations, and has built and led multidisciplinary teams to improve the efficient, safe and secure delivery of healthcare.

Mike's team received the honor of being among the Top 5 Best Hospital IT Teams according to HealthcareITNews in both 2015 & 2017. Other team achievements include CSO Media's CSO50 Award for security initiatives among the top 50 across all industry sectors, recognition by AHA and Hospitals & Health Networks as a Most Wired hospital in 2017, and being named a 2018 winner of the AAMI Foundation & Institute for Technology in Health Care's Clinical Solution Award for meeting the challenge of supporting and securing medical devices and systems. Mike led Beebe Healthcare's two-year journey to receive HITRUST CSF Certification for its IT security program. As a direct result of how the EHR was implemented, Beebe achieved HIMSS Analytics EMR Adoption Stage 6 status (from Stage 3) and won Cerner's Consulting Project Excellence Award Q1 2014.

Before joining Beebe, Mike worked with Robert Wood Johnson University Hospital in NJ for 14 years. He holds a Bachelor of Science degree in Finance from Rider (College) University in Lawrenceville, NJ, and an MBA with a focus in Technology Management from University of Phoenix. He is an active member of the College of Healthcare Information Management Executives (CHIME), earning recognition as a CHIME Certified Healthcare Chief Information Officer (CHCIO) and achieved the distinction of a CHIME Fellow (FCHIME). He is also a Fellow Member of the Healthcare Information Management Systems Society (FHIMSS) and a HIMSS Certified Professional in Healthcare Information Management Systems (CPHIMS).

In February 2016, Mike was appointed to the Governor's Delaware Cyber Security Advisory Council (DCSAC) to represent Delaware's healthcare sector. He also created and chairs the Delaware Healthcare Cyber Security Alliance, comprised of all Delaware hospitals, and the Delaware Health Information Network which works with healthcare practices to share information and threat intelligence. Other membership include: Board of Directors of The Delaware Foundation for Science and Math Education (DFSME), the Delaware Technical Community College's Board of Trustees' Technology Board Committee, the Delaware Technical Community College Technology Advisory Board, and the Cape Henlopen High School Career and Technology Education Advisory Council. He participates in CHIME's Membership Committee, is a member of the NJ HIMSS Security, Privacy and Compliance Task Force, a member of the CommonWell Advisory Board, and a charter provider member of the Sensato/Divurgent Medical Device Cybersecurity Task Force. Mike also participates on the Healthcare Sector Coordinating Council's Medical Device and Healthcare IT Joint Strategic Plan Task Group 1B, (formerly the HHS CISA 405(d) Task Force (Section 405(d) of the Cybersecurity Information Sharing Act of 2015)), and Association for Executives in Healthcare Information Security's (AEHIS) Medical Device Cybersecurity Committee.

Mike founded and is the Chairman of Sussex County STEM Alliance, Inc. comprised of educators, industry, legislators and families to work together to stimulate student interest in STEM education and career pathways. He recognizes the great gender and minority imbalance in the technology industry and advocates for technology opportunities offered this "non-traditional" demographic by supporting the Million Women Mentors mission to advance women and girls in STEM careers through mentoring.

Heather Flannery, Health Circle Global Lead, ConsenSys; Co-Founder & Board Chair, BiHG, IEEE ISTO; Co-Chair, HIMSS Blockchain Task Force

Heather Flannery is the Health Circle Global Lead for ConsenSys, a leading organization in the blockchain space. She is also Co-Founder and the Board Chair of Blockchain in Healthcare Global ("BiHG"), a new 501(c)6 trade association organized under the IEEE ISTO launching in Q3 2018, FY19 Co-Chair of the global HIMSS Blockchain in Healthcare Task Force, an Innovation Fellow at EP3 Foundation, and an active consultant and speaker. Prior to ConsenSys and BiHG, she founded and led Obesity Prevention, Policy, and Management, Inc. ("Obesity PPM"), an innovative provider of disease management, population health, research administration, and information technology managed services for health systems in the Americas, and an early adopter of distributed ledger technology.

Ms. Flannery has driven continuous business model innovation via technology early adoption throughout her 25-year career as an entrepreneur, technologist, and strategist. She has consulted in the public sector in context of international development, and brings a global health perspective to her initiatives. She is a broad, lateral thinker who applies complex adaptive systems theory to identify,

advance, and course-correct critical path to progress against large-scale macroscopic challenges, focusing in the health sector since 2006.

Due to her personal life experience, Ms. Flannery is intrinsically motivated to impact population health and economic prosperity through non-communicable disease prevention and treatment. She builds mission-driven organizations aligned by shared values: making measurable societal contributions, creating economically sustainable interventions, and prioritizing diversity and inclusion.

Julie Connolly, CISSP, Principal Cybersecurity Engineer, The MITRE Corporation

Julie Connolly, CISSP, is a Principal Cybersecurity Engineer with MITRE. Her 20+ years of cybersecurity experience includes policy, strategy, standards, research, and operations work. She is part of a MITRE team supporting the U.S. Food and Drug Administration (FDA) effort to develop collaborative approaches to manage medical device cybersecurity. She has also supported the Department of Health and Human Services' (HHS) and the Centers for Medicare and Medicaid Services' (CMS). She has led MITRE's internal Cybersecurity Operations Team, led several MITRE cybersecurity research projects and vulnerability assessment efforts, led and participated in several cybersecurity standards efforts, including the Common Malware Enumeration (CME), Structured Threat Information eXpression (STIX), and Trusted Automated eXchange of Indicator Information (TAXII) efforts.

Ronnie Daldos, CISSP, MITRE Corporation

Ronnie Daldos is a Certified Information Systems Security Professional (CISSP) and a Lead Cybersecurity Engineer with MITRE. She has a B.A. in Information Technology and an M.S. in IT Business Analysis. Ms. Daldos is a board member for the New Jersey chapter of HIMSS, a co-chair for the chapter's Security, Privacy, and Compliance committee, and a veteran of the U.S. Air Force.

John Gomez, CEO and founder, Sensato Cybersecurity Solutions

John Gomez is the CEO and founder of Sensato Cybersecurity Solutions. John has gained a reputation as a leading-edge cybersecurity researcher and technologist. He is also a cyber attacker and has direct hands-on experience of bypassing safeguards for critical systems. Demonstrating a diverse professional portfolio, John has served as an Executive Vice President, the Co-President and the Chief Technology Officer of Product Development & Delivery at Allscripts Healthcare Solutions, Inc., as well as Chief Technology Strategy Officer and the Executive Vice President at Eclipsys Corporation and was a former Chief Technology Officer and the Senior Vice President at WebMD Corporation. John has led initiatives in design/development for Microsoft Corporation, where he served as the Managing Consultant, the Lead Program Manager and the Architect for the MicroWarehooe e-Commerce System. In addition to his work with healthcare organizations, John has worked as an advisor, researcher and technologist in the banking and insurance industries. He has worked with small startups to multi-national, billion dollar public companies overseeing teams of 2,000 plus team members. John is often called upon to lecture on product design, leadership and operational excellence and future

trends across industries. He is known as a dynamic and engaging speaker who is able to simplify complex topics and use the power of storytelling to help keep an audience engaged.

Brett J. Warrick, Director of Business Development, Sensato Cybersecurity Solutions

Brett Warrick, is responsible for leading Sensato Cybersecurity Solutions Business Development team and is also involved cybersecurity operations. Brett has a background in medical device security, incident response and threat analysis. Brett is an engaging speaker who brings real world experience to his audiences.

Dr. Susan Conaty-Buck, DNP, APRN, FNP-C
Conference Coordinator and Grant PI

Dr. Susan Conaty-Buck is a certified Family Nurse Practitioner, an Assistant Professor and Informatics Nurse Researcher in the University of Delaware School of Nursing. She practices Primary Care at the University of Delaware's Nurse Managed Health Center where she also serves a nurse informaticist and educator for NP students. Dr. Conaty-Buck holds a Doctor of Nursing Practice and Master of Science of Nursing degrees from the University of Virginia and a BSN from James Madison University. Prior to joining the nursing profession, she worked in Arts Management and holds a BA in Music and an MFA in Management. Dr. Conaty-Buck has taught at JMU, UVA and UConn. She was selected in 2015 as an American Association of Nurse Practitioner's (AANP) Leadership Program Fellow and has been a National Library of Medicine Fellow in BioInformatics. She is a member of the AANP Clinical Practice and Research Committees, President of the Delaware Coalition of Nurse Practitioners, and a member of the National Organization of Nurse Practitioner Faculties. She is an Affiliated Faculty member in Bioinformatics and Data Science majors and faculty for Lerner College of Business' Pocket MBA. She represents UD on the American Medical Informatics Association's Academic Forum and is member of the Delmarva region Board of Directors for the American Nurses Informatics Association. She is a recipient of grant fund to research issues in Healthcare Cybersecurity. Dr. Conaty-Buck has served as a grants reviewer for the Office of the National Coordinator for Health Information Technology (ONC) and been an invited panelist for CMS's work to reduce clinician burden. She is a conference speaker and writer about the use of technology in healthcare to benefit patients and providers. Dr. Conaty-Buck practices patient-centered care and utilizes informatics solutions to encourage patient / practitioner communication and collaboration with a goal of improved health and wellness for each patient.

Conference Sponsors

The mission of the University of Delaware Cybersecurity Initiative (UD CSI) is to establish UD as a **center of excellence** in cyber security that encompasses research, education, workforce training and development, and promotes partnerships among the government, private and academic communities. UD CSI has a strategic focus to serve as the cyber security hub for corporate America with an emphasis on financial services.

Within the University of Delaware, **College of Health Sciences**, research provides an evidence-based foundation for the education of the next generation of thought leaders and healthcare professionals. The College of Health Sciences is also a place where partnerships play a key role in promoting health research and education. High-quality undergraduate and graduate programs, research seed grant programs, and clinical research projects enable us to provide our students with rich classroom, laboratory, and clinical experiences.

Special Thanks

Lynn Fishlock, Program Manager of Professional and Continuing Studies, University of Delaware

Arshiya Khan, Conference Coordination Graduate Assistant, UD Engineering Master's Degree Student,

Beth Casey Halley RN MBA FHIMSS, The MITRE Corporation

Katherine Lakofsky, Director, Professional Engineering Outreach at University of Delaware

Margie Zuk, Senior Principal Cybersecurity Engineer, The MITRE Corporation

Advancing Healthcare Cybersecurity Knowledge

www.pcs.udel.edu/health-cybersecurity