

AdvaMed Cybersecurity Summit

December 12, 2022, 12:00 – 3:45 pm ET

December 13, 2022, 12:00 – 3:45 pm ET

Virtual Event

Monday, December 12

12:00 pm – 12:05 pm

Welcome Remarks

Zach Rothstein, Executive Director, AdvaMedDx

12:05 pm – 12:35 pm

Component Based Cybersecurity for Products

Colin Morgan, Apracity LLC

For medical devices, we must evolve and think about the components in the product and how to securely configure them on an individual basis, otherwise we may be missing things that create future risk. A single product may have dozens of components and without individual focus, how can we ensure the device is properly secured. In this session, we will discuss what component-based security is, what it means and why it is a critical approach in developing safe and secure products.

12:35 pm – 1:05 pm

FDA Regulatory Update

Suzanne Schwartz, Director, Office of Strategic Partnerships and Technology Innovation, Center for Devices and Radiological Health, FDA

FDA will provide an overview of the current state of the Agency's cybersecurity efforts.

1:05 pm – 1:45 pm

Uncomfortable Truths: Recent & Imminent Gamechangers to Medical CyberSafety

Joshua Corman, Vice President, Cyber Safety Strategy, Claroty; Former Chief Strategist, COVID Task Force, Cybersecurity and Infrastructure Security Agency

Healthcare was strained before our recent waves of unpleasantness. Our resilience has been further damaged across material disruptions by rapid evolution in ransomware, a global pandemic, and increasingly brazen adversaries taking advantage of our vulnerability. Our recent crucibles revealed and clarified much - crossing new thresholds regarding public safety, public confidence, and political will for substantive reform. We have a small window to work through our discomfort. History has its eyes on us...

1:45 pm – 2:00 pm

Break

2:00 pm – 2:45 pm

Medical Device Penetration Testing Best Practices

Chris Reed, Director of Digital Health and Product Security Policy, Medtronic

MedTech and its regulators have embraced the value of penetration testing to validate medical devices can resist current threats. However, penetration testing practices and the outcomes still vary greatly. There is an opportunity to mature best practices, specific for medical device penetration testing, to help drive consistency and effectiveness of penetration testing validation of security controls. MDIC is close to releasing a best practices document on medical device penetration testing. This session will share the key themes and updated timeline the document is expected to be released.

2:45 pm – 3:45 pm

Product Security Program Evolution

Chris Kohlios, Cyber Risk Senior Consultant, Deloitte
Nick Sikorski, Senior Manager, Product Security, Deloitte

Product security has evolved significantly over the past decade. Regulators, customers, and the drive of manufacturers to protect patients has resulted in an increase in maturity throughout the product lifecycle. In this session, we will discuss our observations from the field working with global medical device manufacturers. We will share data points and benchmark information on both where the industry is today and where they are setting their north star over the next two to three years. Coming out of this session, attendees will better understand and be able to compare their maturity with respect to others in the industry and the direction of where product security programs are focusing their budgets and roadmaps in the near term.

Tuesday, December 13

12:00 pm – 12:05 pm

Welcome Remarks

Zach Rothstein, Executive Director, AdvaMedDx

12:05 pm – 12:35 pm

Limiting Cyberattack Liability Protection through the SAFETY Act

Brian Finch, Partner, Pillsbury Winthrop Shaw Pittman LLP

This presentation will describe how the SAFETY Act, a federal liability protection statute, can limit or eliminate liability associated with cyberattacks on medical devices. Topics covered will include a primer on the SAFETY Act, the kinds of liability the SAFETY Act limits or eliminates, who can apply for these protections, and how the law fits in with cyber insurance.



12:35 pm – 1:35 pm

Hidden Hospital Vulnerabilities

Benoit Desjardins, MD, PhD, Professor of Radiology and Medicine and Co lead, Arrhythmia Imaging Research Laboratory, University of Pennsylvania

Mike Kijewski, CEO, MedCrypt

Jessica Wilkerson, Cyber Policy Advisor with the All Hazards Readiness, Response, and Cybersecurity (ARC) team, Center for Devices and Radiological Health, FDA

Join us on a cross-industry panel discussing the current state of security in DICOM. The panel will consist of a regulatory perspective, a hospital CIO, a representative from an imaging vendor, and a rep from a PACS vendor.

1:35 pm – 1:50 pm

Break

1:50 pm – 2:50 pm

Lessons Learned from Paylocity's Ongoing Journey into DevSecOps

Randy Horton, Chief Solutions Officer, Orthogonal

Michelle Jump, CEO, MedSec

Bruce Parr, Manager of Developer Security Operations – Information/Application Security Teams, Paylocity

DevSecOps (Development Security Operations) is a key modern engineering method for getting ahead of application security issues and fusing best practices for secure software into the normal flow of an organization's development processes and culture. The Software as a Service (SaaS) industry has been a pioneer in DevSecOps as a result of their needs as cloud-first and digital-first businesses. We in MedTech can learn a tremendous amount to learn about successful DevSecOps from SaaS companies.

In this session, we will have a wide-ranging discussion with Bruce Parr, a DevSecOps expert who has been on a multi-year journey of implementation at the fast-growing and well-regarded SaaS payroll provider, Paylocity. And while payroll processing may not be considered critical infrastructure under the formal definition, try telling that to an entire workforce at a company that doesn't get paid one Friday because their employer's payroll vendor is being held ransom by hackers who have taken control of their computers.

In this wide-ranging conversation, Bruce will walk us through Paylocity's DevSecOps journey: what they've learned about it, how they've implemented it, what the results have been and where they are headed next. Through the conversation, we've tie Bruce's points back to some of the specific needs of MedTech, SaMD, DTx, and connected medical device systems,

Our goal is for you to leave this session with a quiver full of new ideas for how to apply this powerful new cybersecurity approach in your own organization.



2:50 pm – 3:45 pm

Moving Beyond the Baseline: Next Steps for Advancing Cybersecurity Maturity in Health Care

Edison Alvarez, Director, Information Security – Governance, BD

Debra Bruemmer, Senior Manager, Mayo Clinic

Greg Garcia, Executive Director, Cyber Security, Health Sector Coordinating Council

Terry Rice, VP, IT Risk Mgt & CISO of Merck & Co., Inc.

Chris Tyberg, Division Vice President, Chief Information Security Officer, Abbott

The Medical Device Innovation Consortium (MDIC) recently launched the inaugural healthcare cybersecurity maturity benchmark report, revealing numerous opportunities to improve cybersecurity and resilience across the healthcare industry. Join Debra Bruemmer, Senior Manager, Mayo Clinic, Greg Garcia, Executive Director, Cyber Security, Health Sector Coordinating Council, Terry Rice, VP, IT Risk Mgt & CISO of Merck & Co., Inc., and Chris Tyberg, Division Vice President, Chief Information Security Officer, Abbott for an engaging panel discussion on advancing cybersecurity maturity, moderated by Edison Alvarez, Director, Information Security – Governance, BD. Topics will include cybersecurity challenges in healthcare compared to other industries, practical ways organizations can use the benchmark report data and strategies for charting a path toward substantial increases in healthcare's cybersecurity maturity over time.