FDA

CERSI
UCSF-Stanford

CYBERSECURITY SEMINAR SERIES

UCSF-Stanford CERSI-FDA Distinguished Speaker Series on Cybersecurity for Biomedical Engineering

3rd THURSDAY OF EACH MONTH:

9:00am – 10:00am PST
12:00pm – 1:00pm EST

https://pharm.ucsf.edu/cersi/cybersecurity

U.S. FOOD & DRUG ADMINISTRATION

Medical Device Security: Welcome and Introductory Remarks

Kevin Fu, Ph.D.

Acting Director, Medical Device Cybersecurity
Program Director for Cybersecurity, Digital Health Center of Excellence (DHCoE)
FDA/CDRH

The views expressed herein do not necessarily reflect the official policies of any entity (i.e., businesses, individuals, organizations, institutions or the U.S. federal government, particularly, U.S. Food and Drug Administration (FDA), nor does mention of trade names, commercial practices, or any entity imply an endorsement. FDA is not responsible for the contents of any outside information referenced in this document.

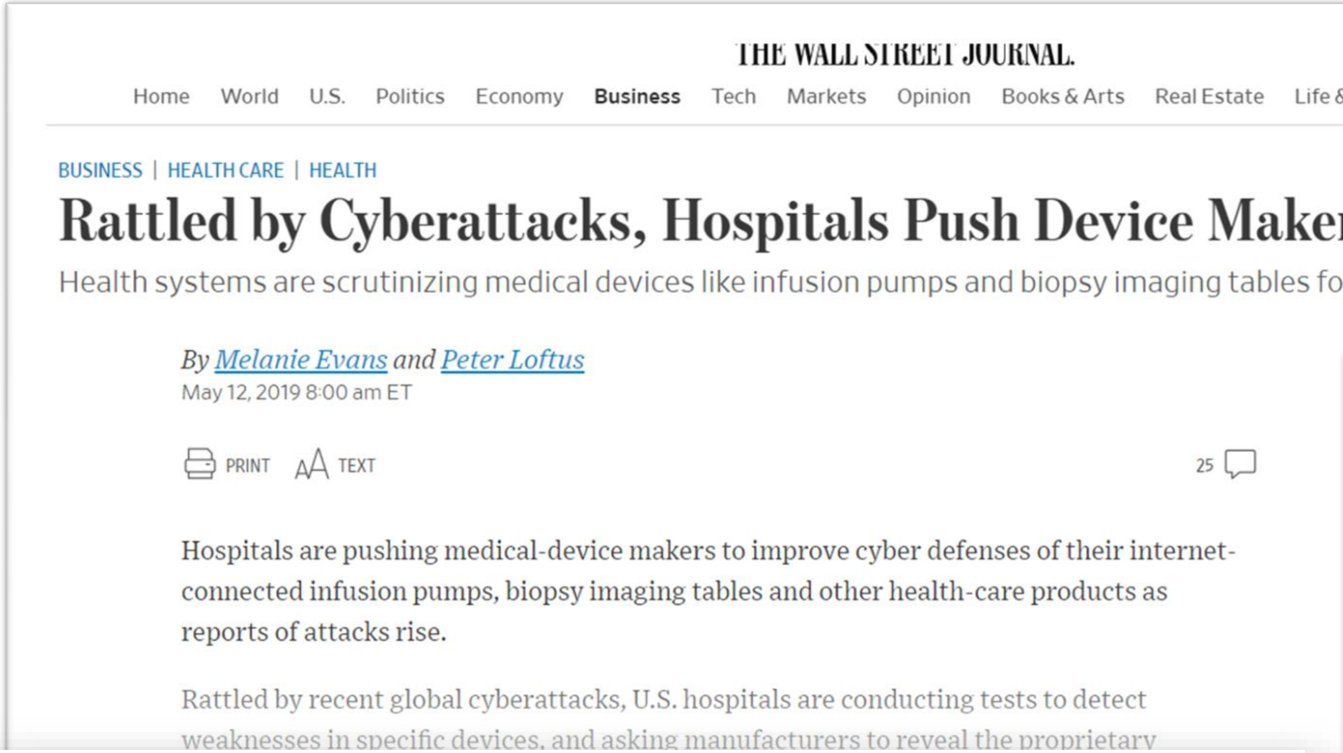
November 2021

Disclaimer

- This seminar series does not represent official FDA policy or guidance. The contents are those of the speaker(s) and do not necessarily represent the official views of, nor an endorsement by, FDA/HHS or the U.S. Government.

- This seminar is recorded. Be aware that this recording will appear on the UCSF-Stanford CERSI public web site.

Why Is Cybersecurity Key for Biomedical Engineering?



THE WALL STREET JOURNAL.

Home World U.S. Politics Economy **Business** Tech Markets Opinion Books & Arts Real Estate Life & Work WSJ. Magazine Sports

Subscribe | S

Search

BUSINESS | HEALTH CARE | HEALTH

Rattled by Cyberattacks, Hospitals Push Device Makers to Improve Security

Health systems are scrutinizing medical devices like infusion pumps and biopsy imaging tables for weaknesses

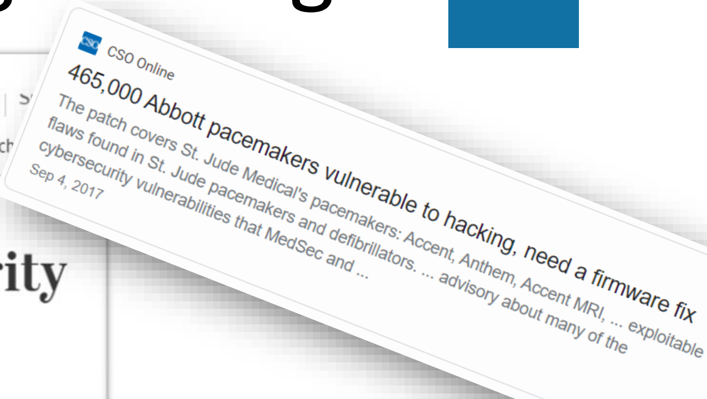
By Melanie Evans and Peter Loftus

May 12, 2019 8:00 am ET

PRINT TEXT 25

Hospitals are pushing medical-device makers to improve cyber defenses of their internet-connected infusion pumps, biopsy imaging tables and other health-care products as reports of attacks rise.

Rattled by recent global cyberattacks, U.S. hospitals are conducting tests to detect weaknesses in specific devices, and asking manufacturers to reveal the proprietary

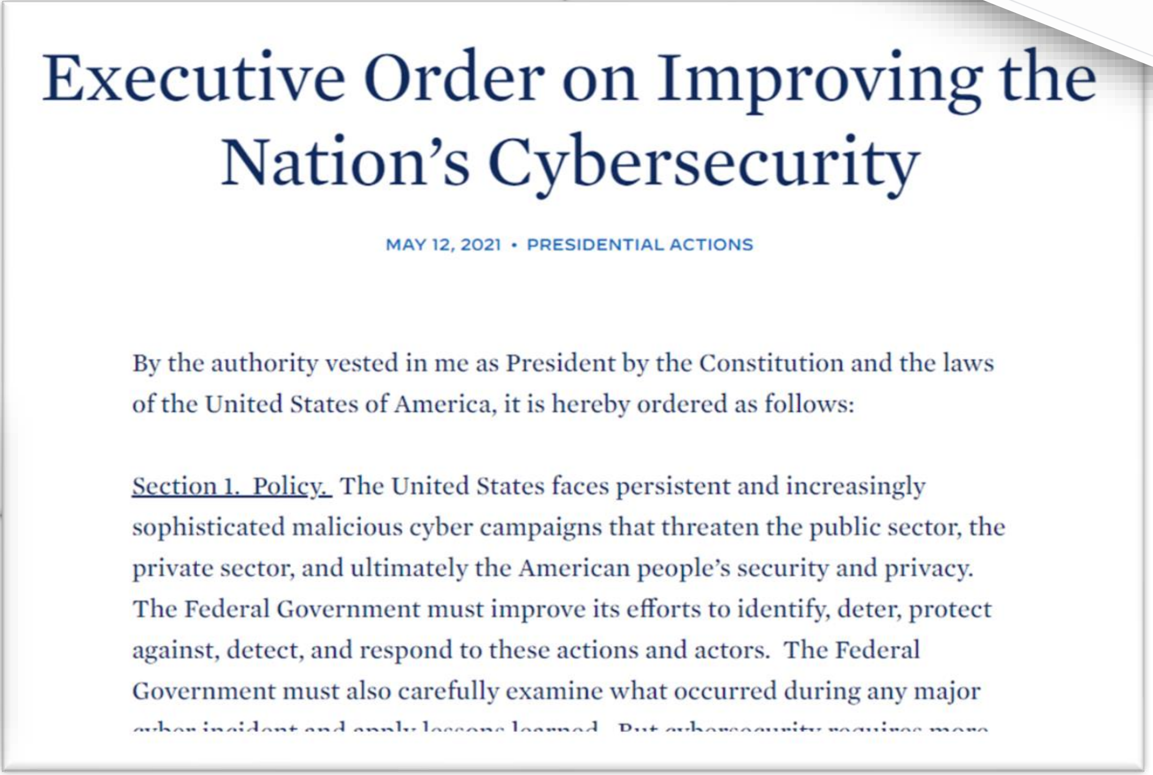


CSO Online

465,000 Abbott pacemakers vulnerable to hacking, need a firmware fix

The patch covers St. Jude Medical's pacemakers: Accent, Anthem, Accent MRI, ... exploitable flaws found in St. Jude pacemakers and defibrillators. ... advisory about many of the cybersecurity vulnerabilities that MedSec and ...

Sep 4, 2017

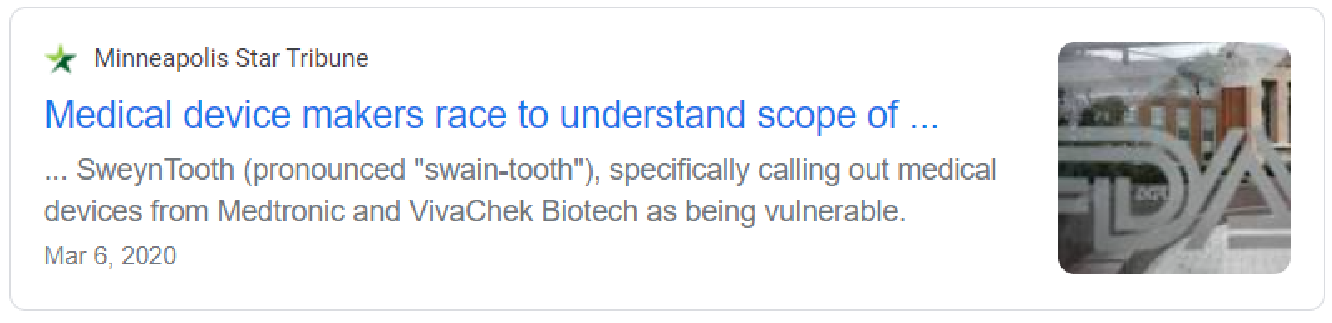


Executive Order on Improving the Nation's Cybersecurity

MAY 12, 2021 • PRESIDENTIAL ACTIONS

By the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

Section 1. Policy. The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. The Federal Government must improve its efforts to identify, deter, protect against, detect, and respond to these actions and actors. The Federal Government must also carefully examine what occurred during any major cyber incident and apply lessons learned. But cybersecurity requires more



Minneapolis Star Tribune

Medical device makers race to understand scope of ...

... SweynTooth (pronounced "swain-tooth"), specifically calling out medical devices from Medtronic and VivaChek Biotech as being vulnerable.

Mar 6, 2020

Distinguished Speaker Series in Cybersecurity for Biomedical Engineering

CERSI
UCSF-Stanford

FDA

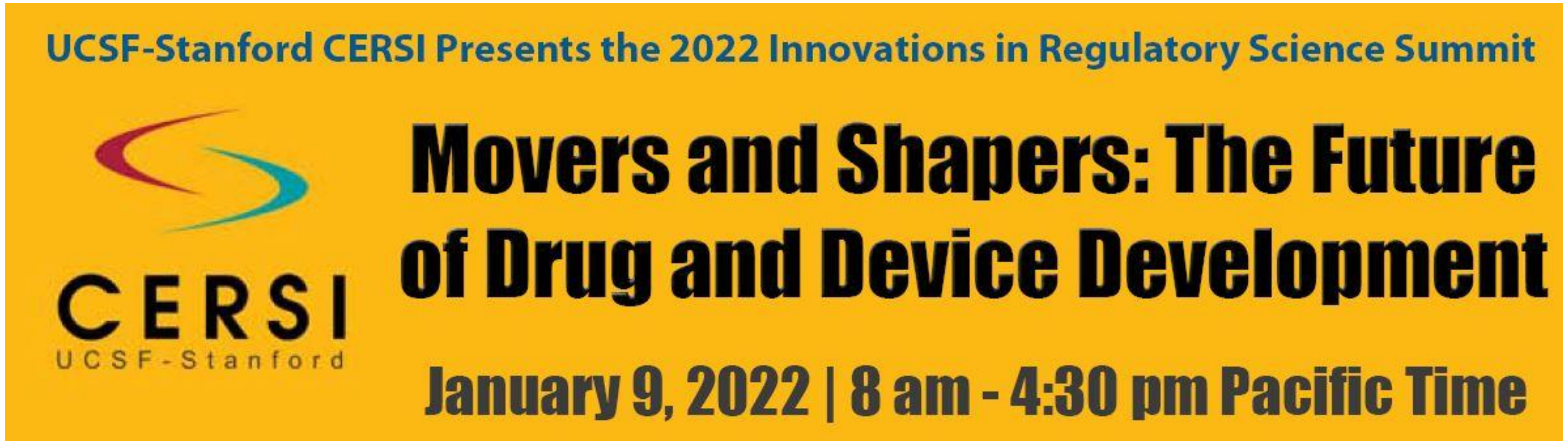
- Presented by the U.S. Food and Drug Administration (FDA) and the University of California San Francisco (UCSF) - Stanford Center of Excellence in Regulatory Science and Innovation (CERSI)

- The one-hour virtual lectures will cover cybersecurity concepts applied to medical devices and biomedical engineering

- Distinguished academic speakers on cybersecurity engineering

UCSF-Stanford CERSI

- FDA-funded regulatory science center at UCSF and Stanford University
  - **Research**: collaborative research projects with FDA scientists
  - **Education**: regulatory science courses, fellowships, scholarships
  - **Outreach**: seminars, meetings, events
- Learn more and join our mailing list at ucsfstanfordcersi.org!



UCSF-Stanford CERSI Presents the 2022 Innovations in Regulatory Science Summit

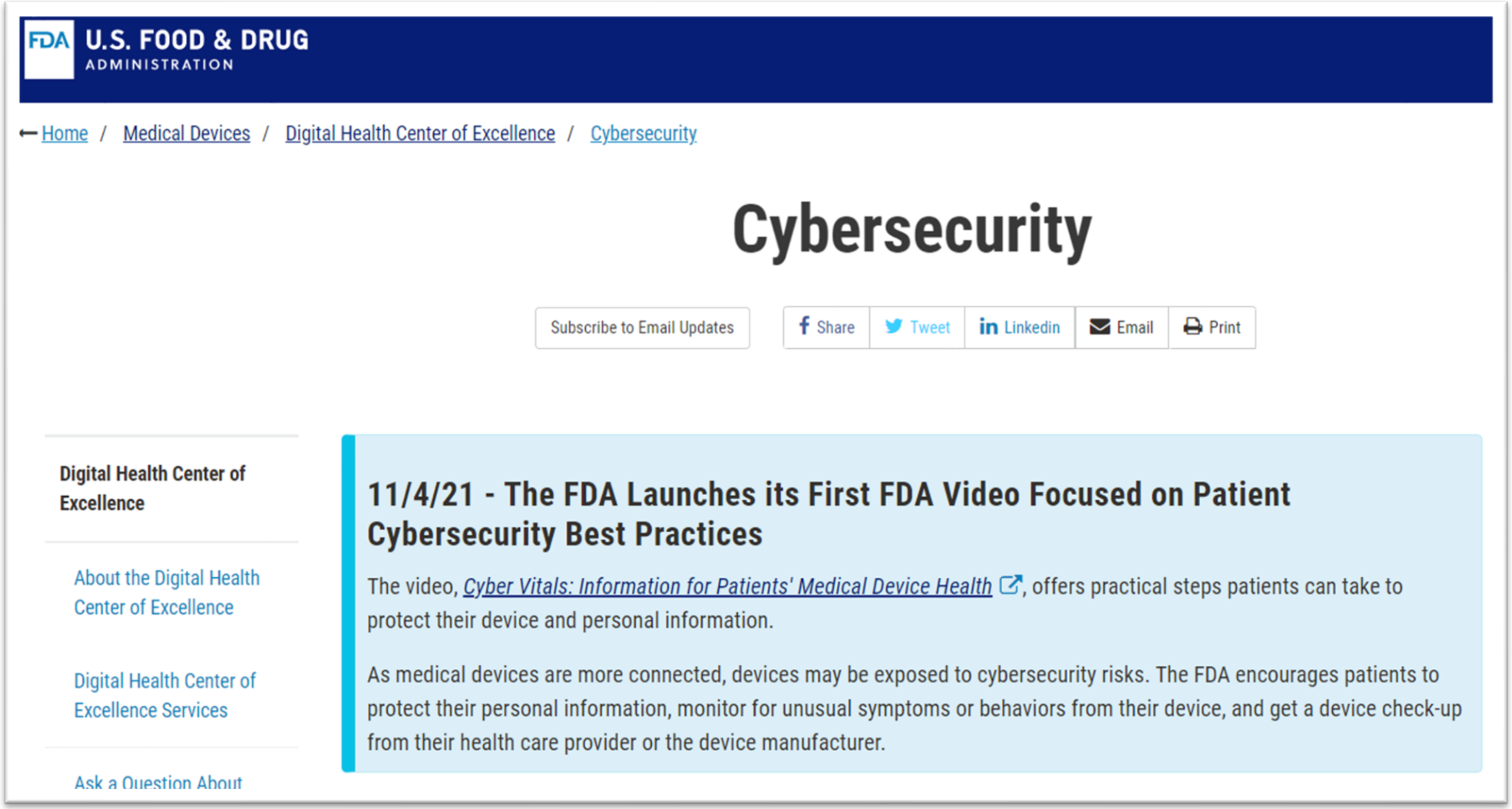
CERSI UCSF-Stanford

Movers and Shapers: The Future of Drug and Device Development

January 9, 2022 | 8 am - 4:30 pm Pacific Time

U.S. FDA Digital Health Center of Excellence

https://www.fda.gov/medical-devices/digital-health-center-excellence/cybersecurity


FDA U.S. FOOD & DRUG ADMINISTRATION
Home / Medical Devices / Digital Health Center of Excellence / Cybersecurity
Subscribe to Email Updates
Share
Tweet
Linkedin
Email
Print
Digital Health Center of Excellence
About the Digital Health Center of Excellence
Digital Health Center of Excellence Services
Ask a Question About

Cybersecurity

11/4/21 - The FDA Launches its First FDA Video Focused on Patient Cybersecurity Best Practices

The video, *Cyber Vitals: Information for Patients' Medical Device Health*, offers practical steps patients can take to protect their device and personal information.

As medical devices are more connected, devices may be exposed to cybersecurity risks. The FDA encourages patients to protect their personal information, monitor for unusual symptoms or behaviors from their device, and get a device check-up from their health care provider or the device manufacturer.

Moderator Bio: Kevin Fu, PhD

- Kevin Fu is Acting Director of Medical Device Cybersecurity at FDA CDRH and Program Director for Cybersecurity in FDA's Digital Health Center of Excellence (DHCoE). He is also Associate Professor of EECS at the University of Michigan. He received his PhD from MIT.
- His publications appear at https://spqrlab1.github.io/publications.html

Upcoming Distinguished Speakers

- December 16: Fred B. Schneider, “*Laws for Cybersecurity,*” The Samuel B. Eckert Professor of Computer Science and Fmr. Department Chair; National Academy of Engineering member, NAE Computer Science and Telecommunications Board member; Founding Chair, National Academies Forum on Cyber Resilience.

- January 20: Lorrie Faith Cranor, *“Security and Privacy for Humans,”* Director and Bosch Distinguished Professor in Security and Privacy Technologies at Carnegie Mellon University, and former Chief Technologist at the Federal Trade Commission.

- TBA: Ross J. Anderson, *“Security Engineering of Machine Learning,”* author of Security Engineering and professor at Edinburgh University + University of Cambridge, UK. Fellow of the Royal Society. Fellow of the Royal Academy of Engineering. Fellow of Churchill College.

Carl Landwehr, PhD

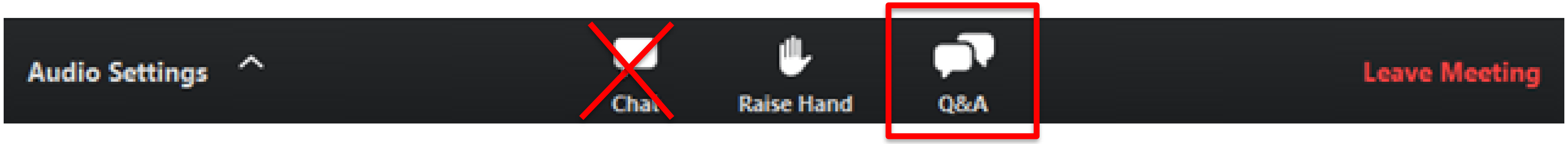
- Today: Carl Landwehr, University of Michigan

- *“Innocence and Experience: Regulatory Tales”*

- Former leader, cybersecurity research programs, National Science Foundation, IARPA, Mitretek Systems and the Naval Research Laboratory. Fmr. editor-in-chief, IEEE Security & Privacy Magazine. IEEE Fellow, NSF Director’s Award for Meritorious Service, Founding Member, National Cyber Security Hall of Fame.

Asking Questions

- Use the Q&A button at the bottom of the Zoom window
  - A popup box will appear where you can send in a question
- Do not use the Chat button
- Submit questions at any time throughout the presentation


Audio Settings
Chat
Raise Hand
Q&A
Leave Meeting