

AAHC President's Council on Cybersecurity

Readiness. Response. Recovery.



Association of Academic Health Centers®

aahcdc.org

AAHC President's Council on Cybersecurity



Robert Barish, MD, MBA Chair	Vice Chancellor for Health Affairs University of Illinois Hospital & Health Sciences System
Lauren Maggio, PhD	AAHC Programs Scholar Associate Professor, Uniformed Services Univ of the Health Sciences
Wilsie Bishop, DPA, MSN	Vice President for Health Affairs East Tenn State Univ Academic Health Sciences Center
Michael Cain, MD	Vice President for Health Sciences, University of Buffalo Dean, Jacobs School of Medicine and Biomedical Sciences
Terri Carrothers	Executive Vice Chancellor for Administration and Finance and CFO Univ of Colorado Denver, Anschutz Med Campus
Michael Diamond, MD	Senior Vice President for Research, Augusta University Associate Dean for Research, Medical College of Georgia
Danny Jacobs, MD, MPH	President Oregon Health and Science University
Adeeba Kamarulzaman, MBBS	Dean of the Faculty of Medicine University of Malaya
Paul Stewart, MD	Executive Dean of the Faculty of Medicine & Health University of Leeds
Richard Thomas, MD, DDS	President Uniformed Services University of the Health Sciences
Walter Tirling	Vice President for Finance and Administration Uniformed Services University of the Health Sciences

Cybersecurity initiatives at AAHC/I

- The **AAHC President's Council on Cybersecurity** has been established and is working toward identifying key cybersecurity issues for CEOs, Deans, and other C-suite leaders at academic health centers.
- The AAHC Annual Meeting on September 25-27, 2019 in Miami will feature an **interactive cybersecurity simulation**, facilitated by Drs. Christian Dameff and Jeffrey Tully, two physician-hackers who will work with attendees to navigate a simulated cyberattack.
- Three curated **case scenarios** and key questions for CEOs, Deans, and other C-suite leaders have been developed by the President's Council.

Cybercrime compromises the patient care mission

- In 2017, at Erie County Medical Center, hackers encrypted the hospital's computer files and demanded payment in bitcoin for their release. Hackers accessed hospital systems using "brute-force" character combinations to crack passwords.
- Operating in a "computer-less" environment, the hospital ran out of paper prescription pads in two days and needed to migrate radiology to plain film. "Digital native" residents were also challenged by the unfamiliar need to write orders and notes in paper charts.

Cybercrime compromises the education mission

- At University College London (UCL) in 2017, a ransomware attack was deployed on the University's student services system. It is believed that hackers gained access to UCL systems, which were protected with up-to-date antivirus software, when a UCL community member navigated to an infected website.
- The attack was timed to coincide with the end of an academic term to generate maximum disruption to students and faculty who found themselves locked out of their accounts and files. As a precaution, several affiliated NHS trust hospitals suspended email accounts to prevent the spread to hospital systems.

Cybercrime compromises the research mission

- In 2018, a global hacking campaign was exposed that operated through coordinated email phishing attempts. These attempts penetrated university accounts of more than 8,000 faculty members in 22 countries at 300 universities, including 144 in the US.
- This illegally-gained access led to the theft of 31 terabytes of data from the contents of faculty inboxes and university systems. The US Department of Justice estimates that \$3 billion in intellectual property was stolen.

Critical Questions About Cybersecurity

- Governance and management
 - Does your institution have in place appropriate team members, and an appropriate reporting structure, to optimize cybersecurity at your academic health center?
- Communications
 - In the event of a cyberattack that compromises email, text messaging, and cell phone capabilities, does your institution's crisis management plan include contingencies to communicate in other ways with leadership, faculty, staff, and learners?
- Cyberdrills
 - Does your institution conduct cyberdrills to improve readiness?
- Cyberinsurance
 - Does your institution maintain cyberinsurance? If so, what is covered and what is not covered by the insurance policy in the event of loss due to a cyberattack?

AAHC President's Councils

AAHC President's Councils are deliberative bodies that examine critical issues facing academic health centers, formulate consensus statements, and share best practices widely in the academic health community. By convening academic health center leaders, individuals with in-depth expertise in a relevant area, and key facilitators, AAHC President's Councils aim to serve as a vital resource for complex and pressing issues facing AAHC/I member institutions.



aahcdc.org