CIO AND INDUSTRY PERSPECTIVE

Cybersecurity Research Acceleration Workshop and Showcase, Indianapolis, IN
October 11, 2017

CIO and Industry Perspective: Panelists

Moderator: Bruce Maas, Innovation Fellow, Internet2

Cynthia Herrera Lindstrom, Vice Provost for IT & CIO, University of Illinois HIPAA Privacy and Security Official

Ed Aractingi, CIO, Marshall University

Julie Johnson, Co-Founder and President, Armored Things

Mark Bruhn, AVP for Public Safety and Institutional Assurance, Indiana University

Mark Henderson, CIO, University of Illinois at Urbana-Champaign

Panel Questions

- Question for Mark Henderson: Mark, you work at a University well known world-wide for being a leader in technology research. What have you been doing as the CIO at Illinois to create opportunities for your staff to engage with researchers, *what is the potential both in general research and in the area of cybersecurity research?*

- Question for Mark Bruhn: You are one of the few individuals in higher education who is responsible both for physical security and cybersecurity. Why has Indiana taken this step to combine these functions under one leader, and what specifically can you do to advance the TTP related to Internet of Things?

- Question for Cynthia Herrara Lindstrom: Cynthia, you are well known in the higher education IT community for your engagement in service. Plus, your campus has a top nationally respected Medical School. How do you envision being of service to researchers, and especially medical researchers, to accelerate cybersecurity research, including perhaps trying out there software in your SOC?

- Question for Julie Johnson: Julie, first tell us a bit about Armored Things. I have observed that you have "bet the house" on your startup company and among other things, are assembling a diverse company right from the ground floor as part of your overall strategy. Why this focus on diversity, and how do you envision that your company could work with cybersecurity researchers and their CIO's as you develop and enhance the capabilities of Armored Things.

- Question for Ed Aractingi: Ed, you've come a fair distance to be with us today. Could you tell us about your engagement with Internet2 related to Internet of Things, and also how you envision working with faculty and companies to create opportunities for cybersecurity research to accelerate?

Sample MOU

- UW Madison Cybersecurity Operations Center, Memorandum of Understanding for Faculty Research

- The University of Wisconsin Madison CIO Office ***encourages collaboration between technology researchers and operations staff***. UW-Madison has one of the most complex learning and research laboratories in the form of its campus network and WAN. We ***encourage researchers to share their research*** with us in the hope that we can ***help them to test out, deploy, and fine tune their intellectual property***. We view this as a win-win scenario.

- In order to ensure the highest level of communication between parties who do have different needs and experiences, it ***is important to write down some of the basic understandings that each party has***. We refer to this as a Memorandum of Understanding. We are in the ***process of developing a boilerplate MOU*** to address some of the most important aspects, and are sharing this with other institutions to create a document which can be of value to other institutions as well.

Sample MOU

1. As part of the Office of Cybersecurity, the Cybersecurity Operations Center (CSOC) has been established to protect the University from cyber-attacks of all forms. As such, it is first and foremost an operations center with a primary mission to protect the university.

2. University ***researchers need environments in which to experiment and innovate***. To the extent that their research can be conducted on the university network ***without compromising operations***, it will be considered.

3. The ***workload and mission needs of the CSOC will take priority*** over the timeline and project needs of the researcher. However, every effort will be made to ***balance expectations so that both needs can be addressed***. We understand that faculty research normally has a timeline, and at times intermediate deadlines, that can create a sense of urgency. ***Discussing key deadlines and expectations up front will minimize disappointment and cross communication***.

4. For research projects that require ***risk assessment and certifications*** (e.g., systems under Federal research programs), ***early contact with the Office of Cybersecurity is required*** to ensure required documentation and testing is complete prior to the project beginning work.

5. If an ***NDA*** is required, this will be ***discussed up front before any research begins***.

6. Staff and student staff will function effectively as extended members of the researcher's team. For that reason, it will be ***important for the researcher and the CISO to build a sense of community*** together. ***This is a partnership***.

7. Within calendar year 2018 the CSOC and Office of Cybersecurity will begin to host a vendor provided service which may be used by researchers in the field of firewalls, intrusion detection and intrusion prevention for research projects.