22ND COLLOQUIUM
FOR INFORMATION SYSTEMS SECURITY EDUCATION

June 13, 2018
New Orleans, Louisiana

# Academic Papers

## ***Paper of the Year:*** *Industry Priorities for Cybersecurity Competencies*

**Michael Whittman**

🕓 11:00 AM to 11:30 AM 📍 La Salle A

With the projected global shortfall of almost 2 million Cybersecurity professionals, it become increasingly critical to promote the development of new Cybersecurity degree programs across the U.S. This raises the question of exactly what should these degree programs prepare students to do? In order to examine this question, this study seeks to identify industry priorities for Cybersecurity competencies based on the Department of Labor's Cybersecurity Industry Model, which creates a tiered set of competencies focusing on the NIST NICE Cybersecurity Workforce Framework categories. The study also seeks to determine if these priorities vary by organizational size or industry.

## ***Student Paper of the Year:*** *Predicting Cyber-Attacks Using Publicy Available Data*

**George Onoh**

🕓 11:30 AM to 12:00 PM 📍 La Salle A

Cyber-attacks are often detected too late. According to reports on reported cyber-attack incidents, most victim organizations do not know that their systems have been breached until they are informed by organizations or individuals external to the victim organization's physical or logical network. This is a significant problem for cyber security professionals and organizations. To further understand this problem, I investigated the following questions in this study: How are external organizations able to detect cyber-attack incidents using only publicly available information? How can cyber-attacks be predicted based on only publicly available data? I collected data on indices representing mentions of a certain type of attack (brute-force / password guessing attack) from public data repositories as well as ground truth data for a target organization. I extracted and stored the data daily. I used the collected data as training data in a machine learning algorithm. After limited training, the system was able to predict future attacks. The results suggest that it is possible to predict cyber-attacks based on publicly available data.