THE UNIVERSITY OF MEMPHIS | Center for Information Assurance

CYBER SECURITY FOR CRITICAL INFRASTRUCTURE WORKSHOP

Summary Report

April, 2022

The Center for Information Assurance (CfIA) successfully hosted the Cybersecurity for Critical Infrastructure workshop on Friday April 1, 2022 on the University of Memphis campus. The hours of the workshop were from 12:00 pm until 5:00 pm. The purpose of the workshop was to highlight the cyber-attacks and other security challenges for emerging information and communication technologies which are continually integrated into national critical infrastructure. A wide variety of topics related to critical infrastructure protection were represented at the workshop which was held both in-person and virtually. The intended audience was state employees, IT professionals, college students, and all persons interested in Cybersecurity within Critical Infrastructures and how to strengthen cyber resiliency. There was participation from various local, state, federal including transitioning workforce. The participants were engaged for five (5) hours on critical infrastructure topics presentations with real-world case studies and market-ready cyber security knowledge, skills for career advancements. At the end of each speaker's presentation, there was time set aside for a question-and-answer segment. The workshop was funded by the Department of Defense (DoD) under the NCAE-C-001-2021 Project Cybersecurity Education for Critical Infrastructure Protection. All participants fully participated at the workshop received completion certificates.

Below is the agenda **of Cybersecurity for Critical Infrastructure Workshop:**

Date: April 1, 2022; 12:00 pm - 5:00 pm

Time	Event
12:00 – 12:10 pm	Welcome Remarks - Dr. Jim McGinnis
	Participants Introduction
12:10 - 12:25 pm	Discussion on Current State of Cybersecurity Dr. Dasgupta
12:25 - 12:50 pm	Cybersecurity Case Studies Review Hampton Roads Sanitation / SolarWinds - (Dr. James McGinnis & Nathan Seymour)
12:50 - 1:00 pm	Break
1:00 – 1:45 pm	Benjamin Denkers, EVP of Operations at CynergisTek. Infrastructure Under Attack: Weaponizing Cyber for Strategic or Tactical Advantage
1:45 – 2:00 pm	Break
2:00 – 3:00 pm	Guest Speaker, Dr Csilla Farkas - U. of South Carolina Cyber-Risk Assessment – a Data-driven View
3:00 – 3:10 pm	Break
3:10 – 3:35 pm	Remote Access Security: Dr. McGinnis Social Engineering, Work from Home.
3:35 – 4:10 pm	Guest Speaker: Jeremy Baker, FBI Memphis Field Office
4:10 – 4:50 pm	Other Security topics & Demo: Defense in Depth - Dr. Dasgupta Zero Trust Model - Nathan Seymour Penetration Testing Demo - Cody Seymour
4:50- 5:00 pm	Questions and Answers / Closing Remarks - Dr. Dasgupta

An underlying objective for the workshop was “Advance your Career in Cybersecurity related profession and opportunities at the University of Memphis”. There was a Pre-Survey, a Post-Survey, and a Post-Survey Assessment given to all participants.

Extracts from the Talks:

The workshop's welcoming remarks were given by the workshop organizer, Dr. James McGinnis. The participants were introduced. Afterwards, Dr. Dipankar Dasgupta conducted an opening talk on 'The Current State of Cybersecurity'. The next presentation segment consisted of case study reviews by Dr. McGinnis and Nathan Seymour. Dr. McGinnis presented information on the Hampton Roads Sanitation ransomware attack. The talk centered on the attack details, the state of the infrastructure, the diagnosis, as well as the remediation and response actions. The presentation was based on research of the Hampton Roads Sanitation District as reported by the podcast '*Ransomware File's* and other related references. Nathan Seymour's presentation centered on the Colonial Pipeline ransomware attack. He also spoke on the SolarWinds and the Kaseya attacks as part of his presentation to the group. In conjunction with the attack incidents, he also presented on research data of key interests points such as: zero trust, zero trust architectures, identity management, access control, and ransomware.

The next segment of the workshop was presented by guest speaker Mr. Benjamin Denkers. The title of the presentation was "Infrastructure Under Attack: Weaponizing Cyber for Strategic or Tactical Advantage". Mr. Denker's presentation focused on the impact cyber security has on critical infrastructures. Disruption as a theme can have an immediate impact as one might imagine; however, the downstream effects of cyber-attacks can be hard to predict and even have worse consequences. Understanding attacker TTPs and how these multipronged attacks evolve, enable organizations to help mature security privacy and security programs to be in the best position to detect and prevent compromises.

After a short break, the next guest speaker was Dr. Csilla Farkas, Professor of Computer Science & Engineering and the Director of Center for Information Assurance Engineering at the University of South Carolina – Columbia. The title of the presentation was "Cyber Risk Assessment – a Data Driven View. The presentation highlights were as follows: Cybersecurity risk assessment methods are hindered by a lack of data availability. Data and information sharing legislation aim to ease this problem. However, the presence of highly sensitive and proprietary data and the lack of mutually trusted entities make such sharing a daunting task. Furthermore, current cyber risk assessment models do not address our nation's social vulnerability to cyberattacks against critical infrastructures. In this presentation we reviewed secure information sharing approaches that may increase the trust in cybersecurity information sharing practices. The speaker suggested a new view on data collection and analysis that is promising to support a multifaceted risk assessment.

The next workshop segment was presented by Dr. James McGinnis, Professor and workshop organizer with the University of Memphis. The title of the presentation was “Infrastructure: Social Engineering, Remote Access, Working from Home”. The highlights of the presentation were the changing threat landscape involving remote home offices, remote access, and social engineering. The presentation included the growing landscape that has evolved over the last two (2) years, predominately due to the Covid19 pandemic. With more employees working remotely, the threat landscape has increased dramatically due to unprepared businesses and home offices without centralized management and/or monitoring of connections and devices.

The next guest speaker for the workshop was Mr. Jeremy Baker, Special Agent in Charge, FBI Memphis Field Office. The presentation title was “FBI Cyber Program and Cyber Investigations. Mr. Baker spoke on the ongoing efforts of the FBI, not only locally, but nationwide, on the increase in cyber activity and the rigor of the investigative involvement of the FBI in cyber-crimes. Working with academia and corporate entities to stay ahead of cyber criminals and keeping the general population informed and up to date on cyber-crime proves to be a fulltime endeavor, as well as a challenge that constantly changes. The presentation touched on many of the efforts and communication activities that are required to stay adept in a changing cyber world. Immediately after Mr. Baker’s presentation, there were two demonstrations conducted by University of Memphis Graduate Students. First Nathan Seymour talked about the Zero Trust Model. Next Cody Seymour did a demonstration on Penetration Testing for the audience followed by questions and/or comments on the student’s presentations.

The last presentation was delivered by Dr. Dipankar Dasgupta, Professor and Director of the Center for Information Assurance with the University of Memphis. Dr. Dasgupta spoke on the status of the Center for Information Assurance and other cyber security highlights. Professor Dipankar Dasgupta’s talk was entitled

"Emerging Cyber Threats such as Ransomware, Targeted Attacks, and APT's Crypto-jacking". He provided some guidelines and best practices in dealing with such cyberattacks from the user's perspective. His talk also covered the importance of Multi-Factor Authentication and ID Management; the concept of Zero Trust, Endpoint Detection and Response, etc. He also discussed various research and educational opportunities available in Cybersecurity at the University of Memphis.

The Cybersecurity for Critical Infrastructure workshop concluded with a question-and-answer segment, at the end of which Dr. Dasgupta gave the closing remarks and encouraged the attendees to check the University of Memphis CfIA's website frequently for upcoming events and workshops being planned.

Workshop Presenter's Biographies:

Mr. Jeremy Baker, Special Agent in Charge, FBI Memphis Field Office. He is the assistant special agent in charge, Intelligence Partner Engagement, Tech Memphis FBI Field Office. In 2020, Mr. Baker earned his certified information systems security professional designation (CISSP) to complement other cyber security certifications he has earned through the FBI's cyber division, Carnegie Mellon university, and SANS. In August 2020, Mr. Baker began work on a master's degree in Cybersecurity Risk Management through Georgetown University, and in 2021, he became a member of the FBI's Adjunct Faculty program, instructing on behalf of the cyber division.

Mr. Ben Denkers is the EVP of Operations at CynergisTek where he is responsible for supporting growth, ensuring effective and efficient service delivery, and achieving the highest levels of client and employee satisfaction in CynergisTek's security, privacy and compliance services. Mr. Denkers has nearly twenty (20) years of experience in information security and consulting that includes markets such as finance, energy, manufacturing, and healthcare.

Dr. Csilla Farkas is a professor in the department of computer science and engineering at the university of South Carolina (UofSC). She is the founder and director of the center for information assurance engineering. Dr. Farkas' research interests include information security, data inference problems, financial and legal analysis of cybercrime, security and privacy on the Semantic web, and information warfare. Her early work pioneered the development of semantics-based security models for web data and metadata. Her most recent work addresses security, privacy, and reproducibility of scientific workflow systems and specific security concerns of High-Performance Computing (HPC) systems. She has published over 100 peer-reviewed conference and journal papers. Her research has been funded by the National Science Foundation, National Security Agency, Space and Naval Warfare, IBM, Federal Railroad Administration, and the South Carolina Department of Commerce.

Dr. Dipankar Dasgupta is Hill Professor of Computer Science and the director of the center for information assurance at the University of Memphis. Dr. Dasgupta is a professor of Computer Science and is the founding Director of the Center for Information Assurance (CfIA), (http://cfia.memphis.edu). The Center has been a National Center for Academic Excellence in Information Assurance Education (CAE-CD since 2004) and in Research (CAE-R since 2010). He spearheads the University of Memphis' education, training, and community outreach activities on Cybersecurity and Information Assurance (IA). Dr. Dasgupta's research covers broad areas of computational intelligence (including AI and machine learning) for the design and development of intelligent solutions. He is one of the founding fathers of the field of artificial immune systems, making major contributions in developing tools for digital immunity and survivable systems. Dr. Dasgupta has published several books and edited volumes including Advances in User Authentication (2017), Immunological Computation (2008), Artificial Immune Systems (1999), and another book on genetic algorithms (1996). Dr. Dasgupta has more than 300 publications. A Google search of his name indicates more than 16,500 citations, and an academic search in Microsoft shows that he has collaborated with 106 co-authors, an extraordinary testimony to the broad influence of his contributions within the research community. With an H-index of over 58, he is featured on UCLA's list of prominent computer scientists.

Dr. James McGinnis is an Assistant Professor in the Herff College of Engineering at the University of Memphis. Dr. McGinnis has over twelve (12) years of experience in Academia, and over twenty (20) years of experience in the corporate world. He has been on the front line of Information Technology while serving as an IT Engineer, IT Manager, IT Security Manager, and IT Department director. He has had experience in security policies, Disaster Recovery, Business Continuity and Training.

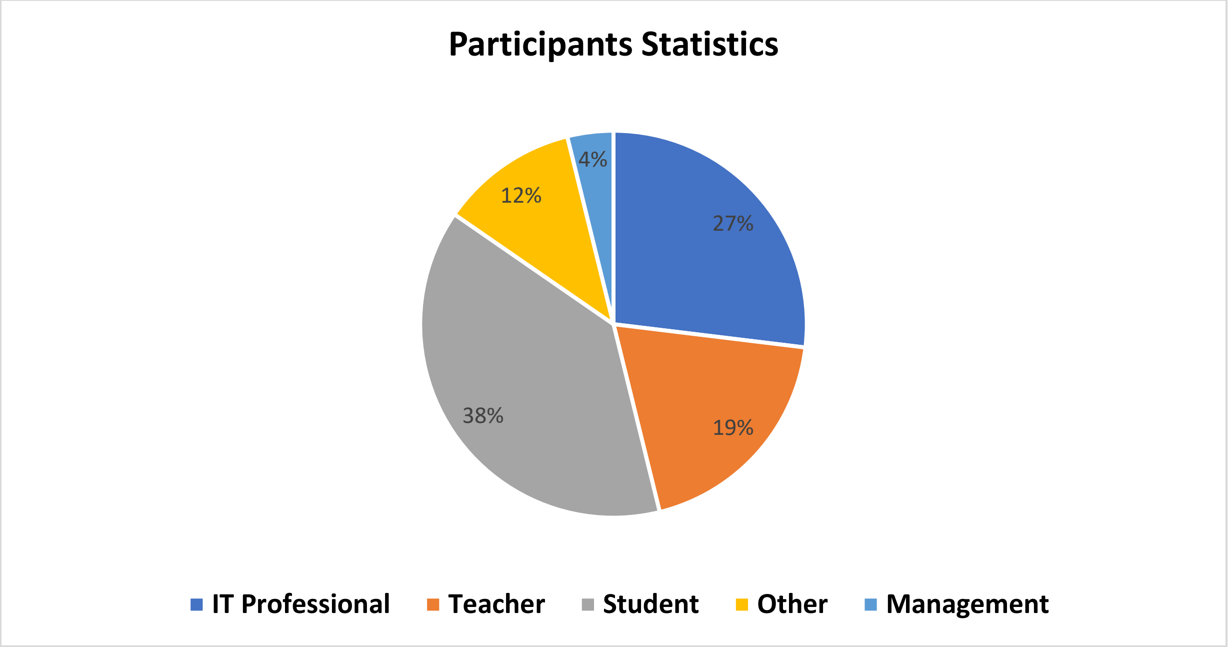
Dr. McGinnis has achieved certifications by ISACA (CISM), Microsoft Server and Workstations, CISCO NetAcademy for the Cisco CCNA series Instructor, and CCNA Cybersecurity. He has extensive training and actual experience in the fields of IT and Security of Information.

Mr. Nathan Seymour is a graduate student in the Computer Science department at the University of Memphis. Currently, he is working under Dr. Dipankar Dasgupta as a graduate research assistant on the Cybersecurity Education for Critical Infrastructure Protection project. Some of his research interests include: Zero Trust, Zero Trust architectures, Identity Management and Access Control, and Ransomware.

Mr. Cody Seymour is an undergraduate student who worked on different security tools and techniques including SNORT intrusion detection system, firewalls, penetration testing and forensic tools.

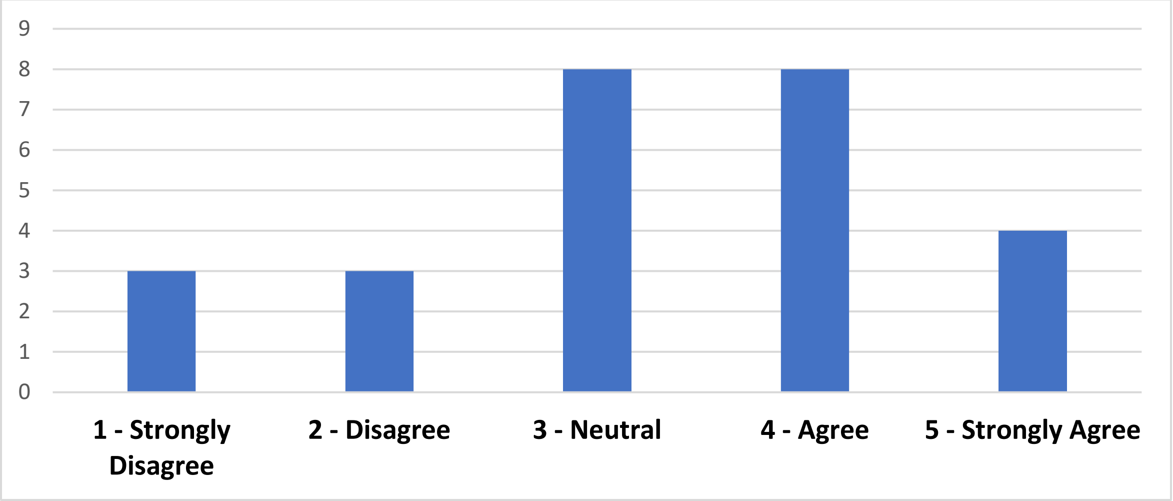
Appendix A: Workshop Participation data and feedbacks.

A total of 71 people registered for the workshop for both face-to-face and virtual event. The following chart depicts the different categories of participating professionals who responded to the survey polls.

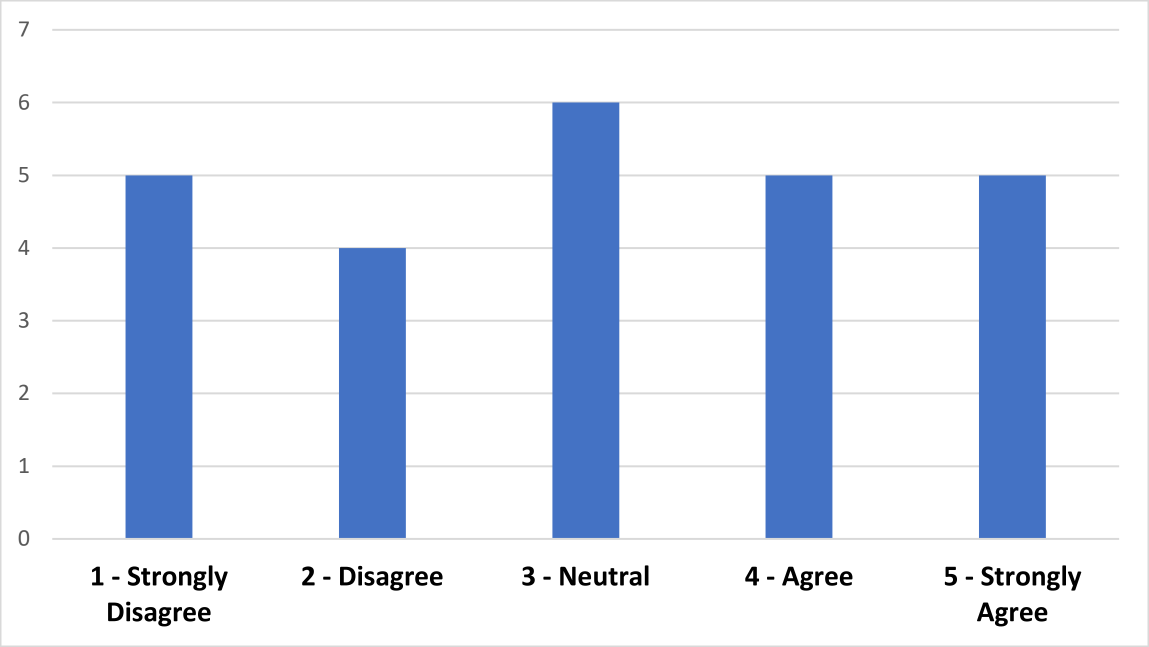


Additional data collected from the attendees as feedback on the workshop and is graphed below:

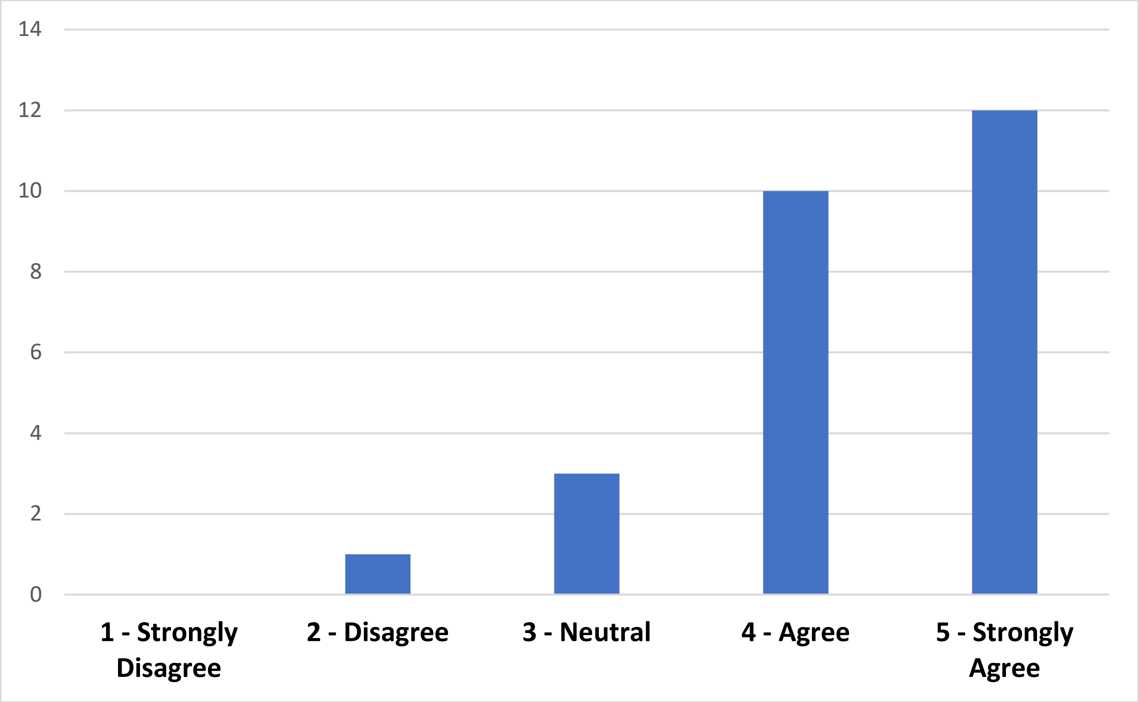
1. The current level of knowledge about cybersecurity for critical infrastructure for the attendees are depicted in the chart below:



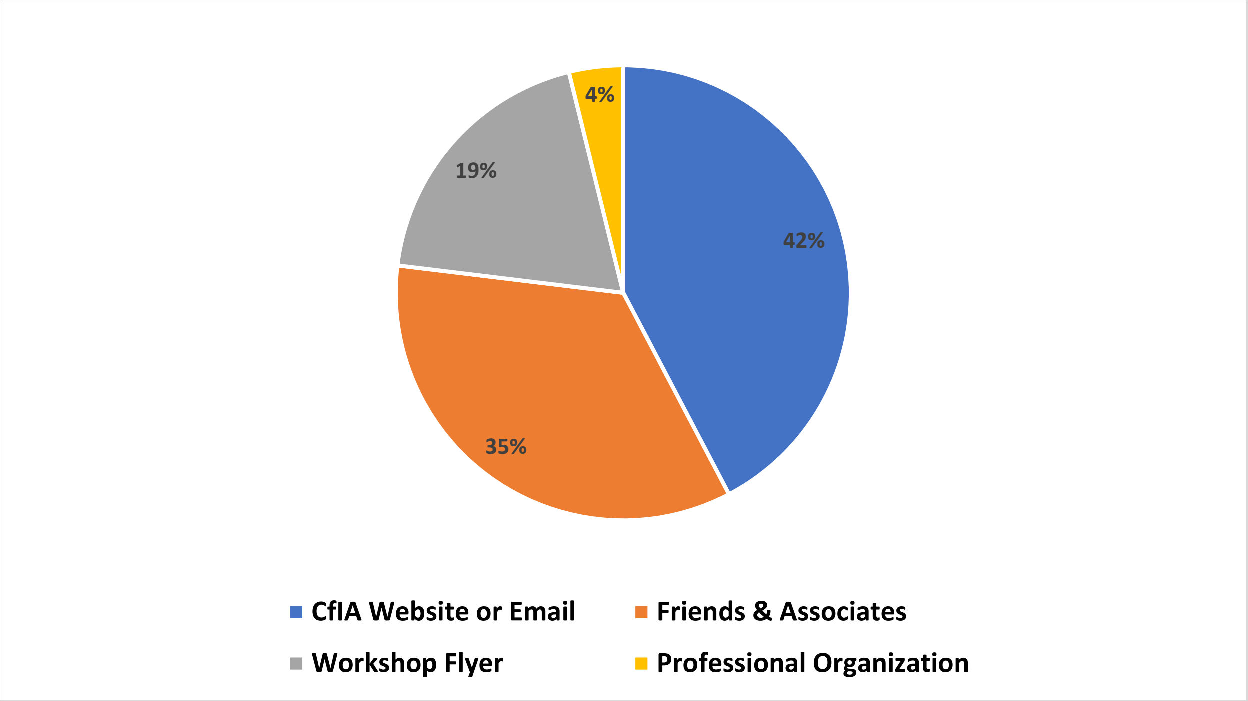
2. Your Employer Provides Critical Infrastructure Training:



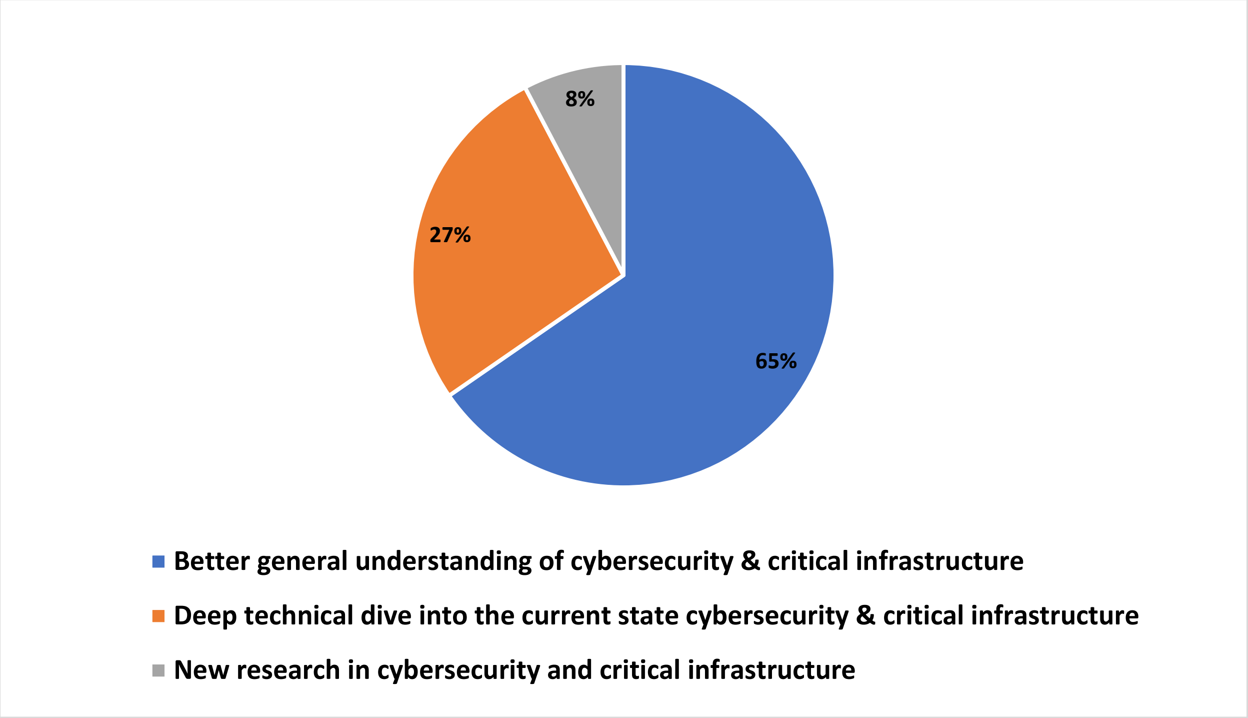
3. A Critical Infrastructure Career Interest You:



4. How did you hear about this Critical Infrastructure Workshop?



5. Your Expectations for this Critical Infrastructure Workshop:


Better general understanding of cybersecurity & critical infrastructure
Deep technical dive into the current state cybersecurity & critical infrastructure
New research in cybersecurity and critical infrastructure