CYBERSECURITY FOR CRITICAL INFRASTRUCTURE WORKSHOP

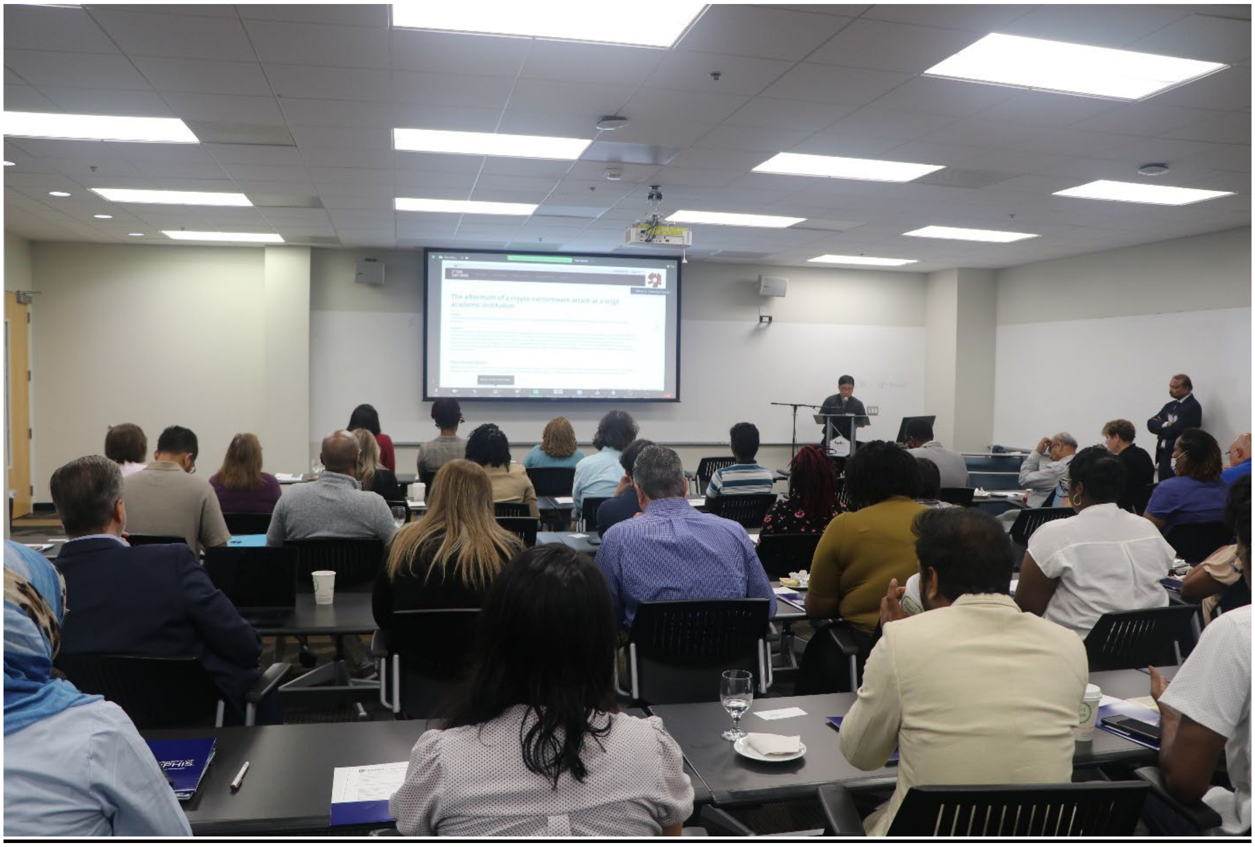


FIGURE 1: CYBERSECURITY FOR CRITICAL INFRASTRUCTURE WORKSHOP

Date and Venue

The University of Memphis Center for Information Assurance (CfIA) hosted the “Cybersecurity for Critical Infrastructure” workshop on June 10, 2024. The event was held in the Fishbowl Room of the FedEx Institute of Technology. The hybrid-formatted workshop attracted seventy-three participants (i.e., 50 in-person, 23 virtual) and covered a wide range of topics centered around cybersecurity for critical infrastructure.

Workshop Team

Dr. Myounggyu Won, Associate Professor of Computer Science, served as the event coordinator in conjunction with Dr. Dipankar Dasgupta, Professor and Director of the CfIA, and Dr. Mohd Hasan Ali, Professor of Electrical/Computer Engineering. Team members Doris Allen, Debera Pittman, and Francis Smith helped with in-person attendance check-in, gift bags, and raffle drawings. Research Assistant Professor Dr. Arunava Roy and Project Coordinator Tony Pinson helped with virtual attendance check-in and workshop facilitation.

Several student workers helped with the workshop as well. Undergraduate Aniqa Ali helped with the raffle drawings whereas Md Nahidul Islam, a computer science graduate student and teaching assistant, served as the photographer for the event.

The workshop team or host committee is shown in the photo below.

FIGURE 2: UOFM FACULTY, STAFF, AND STUDENT WORKER HOST COMMITTEE

Agenda

The workshop opened with remarks from Dr. Dipankar Dasgupta, Professor and Director of the Center for Information Assurance (CfIA), and Ms. Karen Bell, Associate Chief Information Officer for the University of Memphis (UofM). Dr. Myounggyu Won, Associate Professor of Computer Science, was the moderator for the event.

It should be noted that speaker Matthew Collin, a Citadel College graduate student, did not attend due to a scheduling conflict. As a result, his presentation on “Assessing and Ranking Vulnerabilities in Industrial Control Systems” is omitted from the workshop presentation summaries.

The workshop agenda is shown below.

Workshop Agenda	
09:00 - 09:30 AM	Welcome by Dr. Dipankar Dasgupta and Dr. Myounggyu Won
09:30 - 10:00 AM	Dr. Jacqueline Clare Mallett (Reykjavik University, Iceland), In the Aftermath of a Ransomware Attack
10:00 - 10:30 AM	Matt White (Baker Donelson), Current Cyber Threats Facing Critical Infrastructure (with Real World Examples)
10:30 - 11:00 AM	Dr. Guillermo Francia (University of West Florida), Open Platform Infrastructure for Industrial Control System Security
11:00 - 11:30 AM	Bryan McCloskey (FBI), FBI's Mission in the Cyberspace, Tools and Resources
11:30 - 12:00 PM	Matthew Collins (Citadel), Assessing and Ranking Vulnerabilities in Industrial Control Systems
12:00 - 01:00 PM	Lunch Break
01:00 - 01:30 PM	Dr. Richard Maiti (Kentucky State University), Privacy and Security Matters Related to Use of Mobile Devices and Social Media
01:30 - 02:00 PM	Panel Discussion (Dr. Dipankar Dasgupta, Dr. Hasan Ali, Mr. Bryan McCloskey, Moderator: Dr. Myounggyu Won), Challenges and Solutions for Cybersecurity for Grid Systems and AI
02:00 - 02:30 PM	Hans Siegfried Amelang (University of Memphis), Cybersecurity Threats and Solutions for Satellite Communication
02:30 - 03:00 PM	Stoddard A Katherine (Arkansas State University - Mid South), Smart Home and Smart Grid: Threats and Countermeasures
03:00 - 03:30 PM	Raffle Drawing
03:30 - 04:00 PM	Closing Remarks (Dr. Dipankar Dasgupta)

Workshop Presentation Summaries

In the Aftermath of a Ransomware Attack
Dr. Jacqueline Clare Mallet (9:30 am – 10:00 am)

Summary: Dr. Mallet, a cybersecurity professor at Reykjavik University in Iceland, shared insights into a recent ransomware attack on the university orchestrated by Akira, a Ransomware-as-a-Service (RaaS). The attack targeted students and employees, emphasizing the urgency for improved security protocols. Dr. Mallet identified a lack of collaboration between the IT and Computer Science departments as a contributing factor to the attack's success. The university disclosed the breach three weeks after its occurrence. Exploiting CVE-2023-20269, Akira gained initial access by seeking logins and credentials, causing a system-wide shut down for several days. Despite utilizing Linux systems, the attack disrupted operations. While some data was exposed, not all individuals were affected. The attackers focused on compromising backups, including NAS devices, prompting the NCSC-FI to recommend offline backups following the 3-2-1 rule. Compromised online backup systems complicated recovery efforts. The Q&A session highlighted inquiries about cybersecurity insurance payouts and cooperation, emphasizing the necessity for improved security measures and communication within the university.

Current Cyber Threads Facing Critical Infrastructure (with Real World Examples)
Matt White (10:00 am – 10:30 am)

Summary: Mr. Matt White addressed the profound impact of cyber threats, often stemming from human errors. He highlighted the increasing prevalence of zero-day attacks, exemplified by the incident targeting MOVEit file transfer. Notable breaches at Caesars/MGM resulted in substantial financial losses, with 8K filings and class action lawsuits ensuing. Additionally, Change Healthcare encountered a $25 million loss due to a deep fake attack, where only one attendee in the meeting was genuine.

The cybersecurity landscape is evolving swiftly, marked by advanced technology, sophisticated attacks, and heightened regulations. White stressed the importance of effective incident response plans, citing potential savings averaging $1.5 million for organizations. Involvement of law enforcement is pivotal, with non-cooperating entities facing additional costs averaging $470,000. He referenced the Stuxnet virus, a 2010 worm targeting PLCs, to underscore the gravity of cyber threats.

Mr. White highlighted that data exfiltration occurs in 80% of attacks, with zero-day attacks in vendor supply chains showing an upward trend. The average cost of data breaches stands at $9.48 million in the U.S. and $4.35 million globally, with an average identification and containment duration of 277 days. Organizations equipped with incident response plans enjoy a 58% reduction in costs compared to those without. In 2023, global cyber-attacks occurred at a rate of 13 per second, significantly affecting critical infrastructure.

Open Platform Infrastructure for Industrial Control System Security
Dr. Guillermo Francia (10:30 am – 11:00 am)

Summary: Dr. Francia, a professor at the University of West Florida, discussed various aspects of industrial control systems (ICS). He presented an affordable infrastructure for effective ICS security training, providing valuable insights into the design and implementation of the ICS Open Platform Infrastructure (OPI). This platform facilitates the validation of new ICS vulnerability assessment and security testing tools. Containers can easily be shared and run on multiple hosts, ensuring usability across different environments.

Dr. Francia outlined the design guidelines for the ICS Open Platform Infrastructure, emphasizing the role of Human-Machine Interface (HMI) and sandboxed operational technology (OT) network architecture. He highlighted the collaboration with security purple teams to perform activities such as reconnaissance, lateral movement, deep packet inspection, ICS packet crafting, digital forensics, threat hunting and intelligence, and intrusion detection and prevention.

FBI's Mission in the Cyber Space, Tools, and Resources
Mr. Brian McCloskey (11:00 am – 11:30 am)

Summary: Mr. McCloskey introduced himself and his colleagues, discussing the activities of threat actors and the importance of protecting critical infrastructure. He highlighted cybersecurity trends, including investment schemes, double extortion, phishing attacks, supply chain vulnerabilities, and IoT threats. His department oversees the Cryptocurrency Task Force in Memphis, Tennessee.

Mr. McCloskey noted that 40% of cybersecurity breaches occur through the supply chain. Key vulnerabilities in critical infrastructure include legacy systems, lack of security awareness, reliance on third-party vendors, insufficient training, and BYOD (bring your own device) policies. The FBI is actively providing training and intelligence, with their Recovery Asset Team achieving a 71% success rate. They leverage global partnerships for investigations and work to dismantle threat actors' infrastructure.

Emerging threats include quantum computing, AI-driven attacks, ransomware, and the convergence of physical and cybersecurity risks. The FBI has dismantled 18 cybercriminal operations and secured 167 convictions, targeting groups like Qakbot, Genesis Market, and the Snake malware group.

Privacy and Security Matters Related to Use of Mobile Devices and Social Media
Dr. Richard Maiti (1:00 pm – 1:30 pm)

Summary: Dr. Maiti discussed the use of mobile devices and social media, noting that people spend an average of 2 hours and 22 minutes on their mobile devices daily. These devices, used to connect to the internet, can become attack vectors through installed applications and internet browsers. Common threats include phishing, financial data theft, fake requests, brand impersonation, and ransomware. Adults expressed significant concerns about privacy and security on platforms like Facebook.

Key vulnerabilities arise from sharing locations, indiscriminately accepting cookies, and using public Wi-Fi. Weak passwords and reusing passwords can also lead to security breaches, as can downloading applications or media from unsecured URLs. Dr. Maiti recommended using VPNs but warned about the risks of man-in-the-middle attacks and rogue Wi-Fi networks.

Panel Discussion: Challenges and Solutions for Cybersecurity for Grid Systems and AI
Dr. Dipankar Dasgupta, Dr. Hasan Ali, Mr. Bryan McCloskey, Moderator: Dr. Myounggyu Won)

Summary: Dr. Won introduced each panelist: Dr. Dipankar Dasgupta, Dr. Hassan Ali, and Mr. McCloskey. Each panelist brought expertise in cybersecurity about artificial intelligence (AI), smart power grids, or law enforcement. Dr. Dasgupta stressed the importance of demystifying artificial intelligence. Black box artificial intelligence methods or pre-trained models have become too commonplace. He emphasized the need for broader training data coverage and deeper algorithmic analysis to help address their vulnerabilities more effectively. Dr. Ali emphasized the increasing vulnerability of power grids as they transition to smart grids connected to the Internet. He highlighted the threat that hackers pose to SCADA Electric Operations (i.e., manipulating voltage levels, power cycles, and circuit breakers).

AI & Cybersecurity
➢ AI is Computational Logic, Not Magic!
➢Success hinges on the breadth and depth of Training Data Coverage ☺
➢ Pre-trained Models are vulnerable to Attacks ☹

FIGURE 3: PANEL DISCUSSION DURING MID-AFTERNOON BREAK

Cybersecurity Threats and Solutions for Satellite Communication
Hans Siegfried Amelang (2:00-2:30 PM)

<u>*Summary:*</u> The discussion delved into the cybersecurity landscape, emphasizing the crucial aspects of security and reliability in low Earth orbit (LEO) satellite communication systems. These systems orbit at low altitudes, typically between 500 to 2000 km, with orbit periods of 90 to 100 minutes, boasting low latency of 30-50ms compared to Geostationary Earth Orbit (GEO) satellites with 200ms+ latency. Despite their cost-effectiveness in production and launch, LEO satellites face challenges due to limited resources and capabilities.

The presenter outlined the security and reliability requirements imperative for LEO satellites, addressing both active and passive risks such as eavesdropping, satellite transponder theft, and privacy breaches. The classification of these risks was discussed along with potential mitigation strategies. Passive security solutions like spread spectrum jamming suppression (DSSS, FHSS, etc.) and advanced security-oriented antennas aimed at fortifying LEO satellite systems against vulnerabilities were among the alternatives.

Smart Home and Smart Grid: Threats and Countermeasures
Stoddard A Katherine (2:30-3:00 PM)

Summary: The speaker provided a comprehensive overview of both the advantages and challenges associated with basic smart home devices. On the positive side, these devices offer enhanced convenience, promote clean energy usage, bolster security, and contribute to sustainability efforts. However, they also come with drawbacks such as budget constraints, demanding technical requirements, and compatibility issues with legacy infrastructure.

In addition to highlighting the benefits and limitations, the speaker discussed strategies for optimizing electrical consumption, enhancing automation capabilities, and facilitating monitoring within smart homes and smart grids.

Furthermore, the discussion underscored the potential threats facing such systems, including susceptibility to natural disasters and cyber-physical attacks. Maintenance concerns were also addressed, emphasizing issues like the absence of robust cybersecurity support, inadequate visibility into system operations, and the expanding threat landscape.

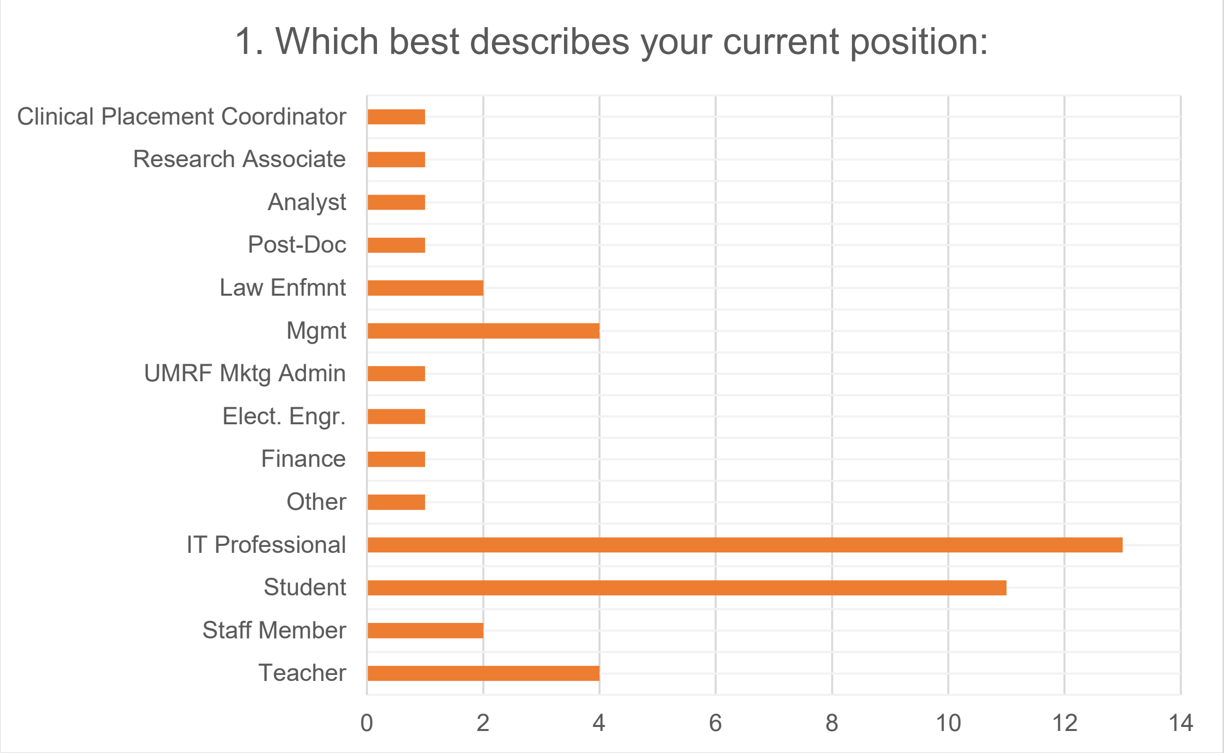
Conclusion

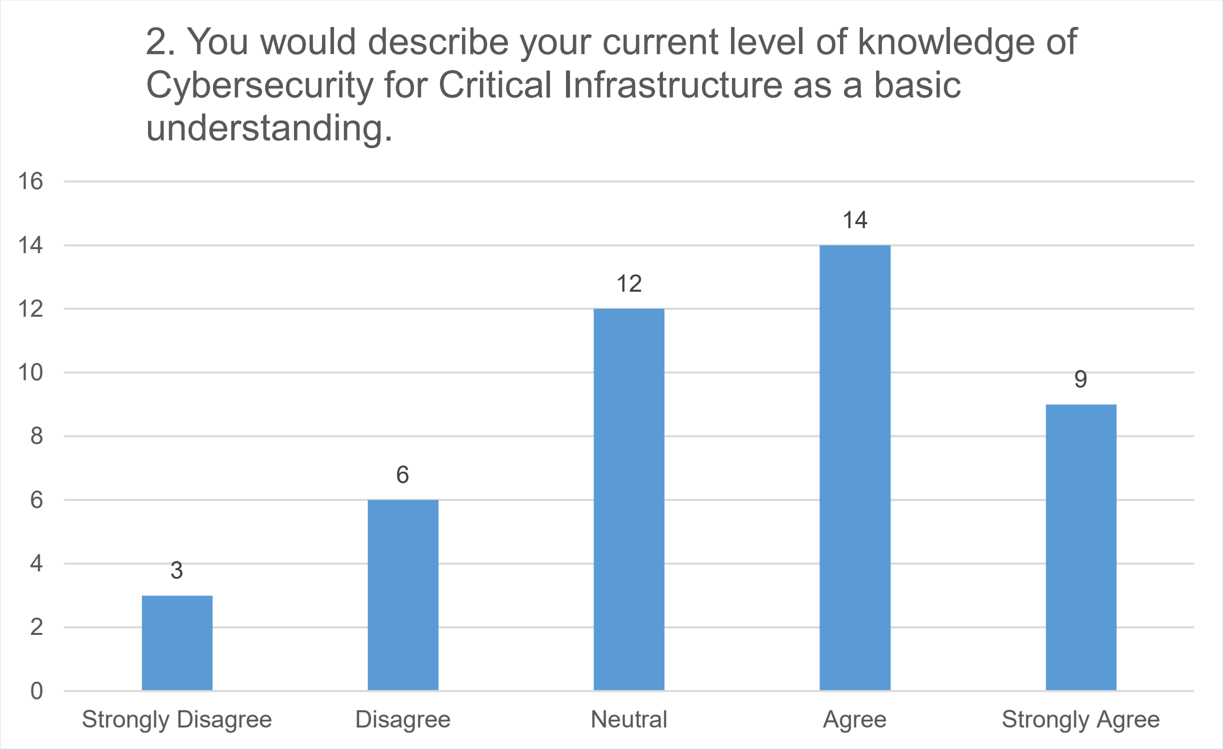
The marketing and implementation of the workshop was very successful. The hybrid format workshop garnered seventy-three participants out of the 95 that registered. Moreover, forty-four of the attendees completed and submitted their surveys. Roughly 28 survey participants were management, IT professionals, or students.

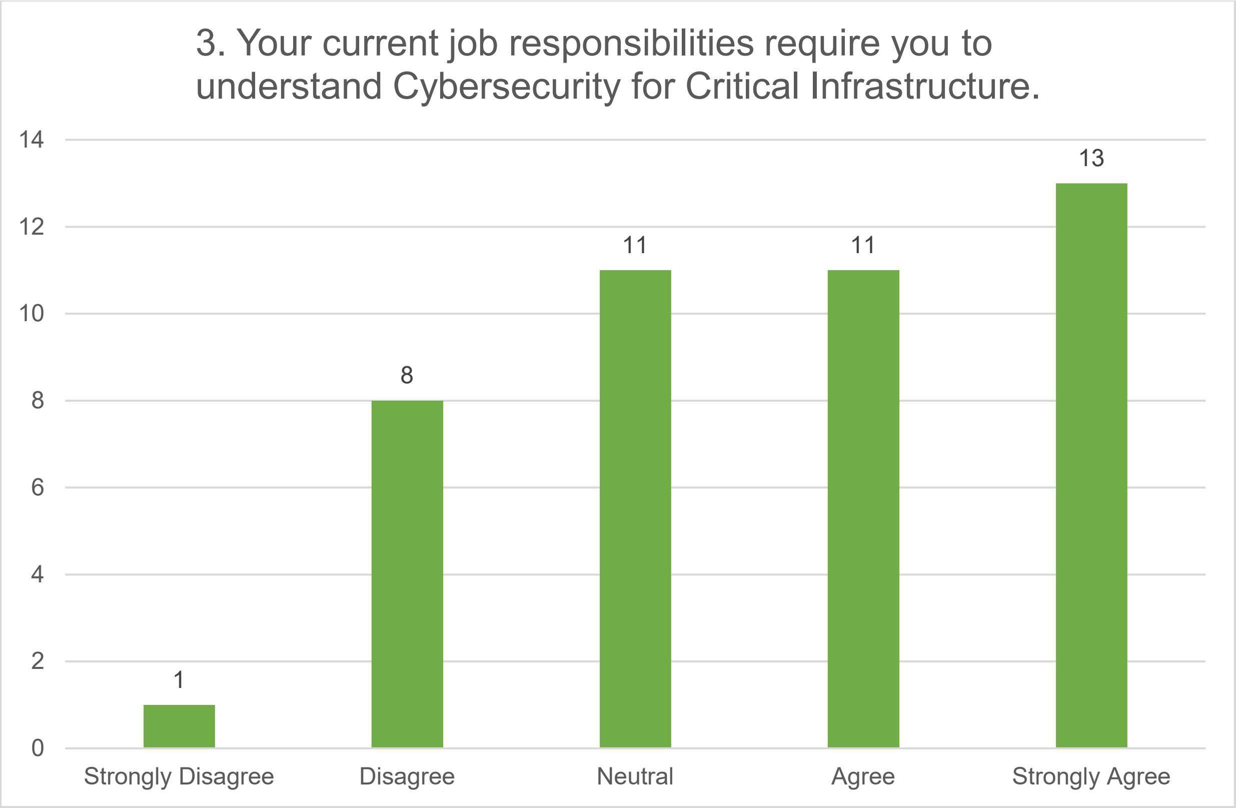
The workshop presentations were received well also. Roughly 80% of the participants surveyed before the workshop indicated that they felt like they had a fundamental understanding of critical infrastructure cybersecurity. Moreover, the same percentage indicated that their current jobs required an understanding of cybersecurity.

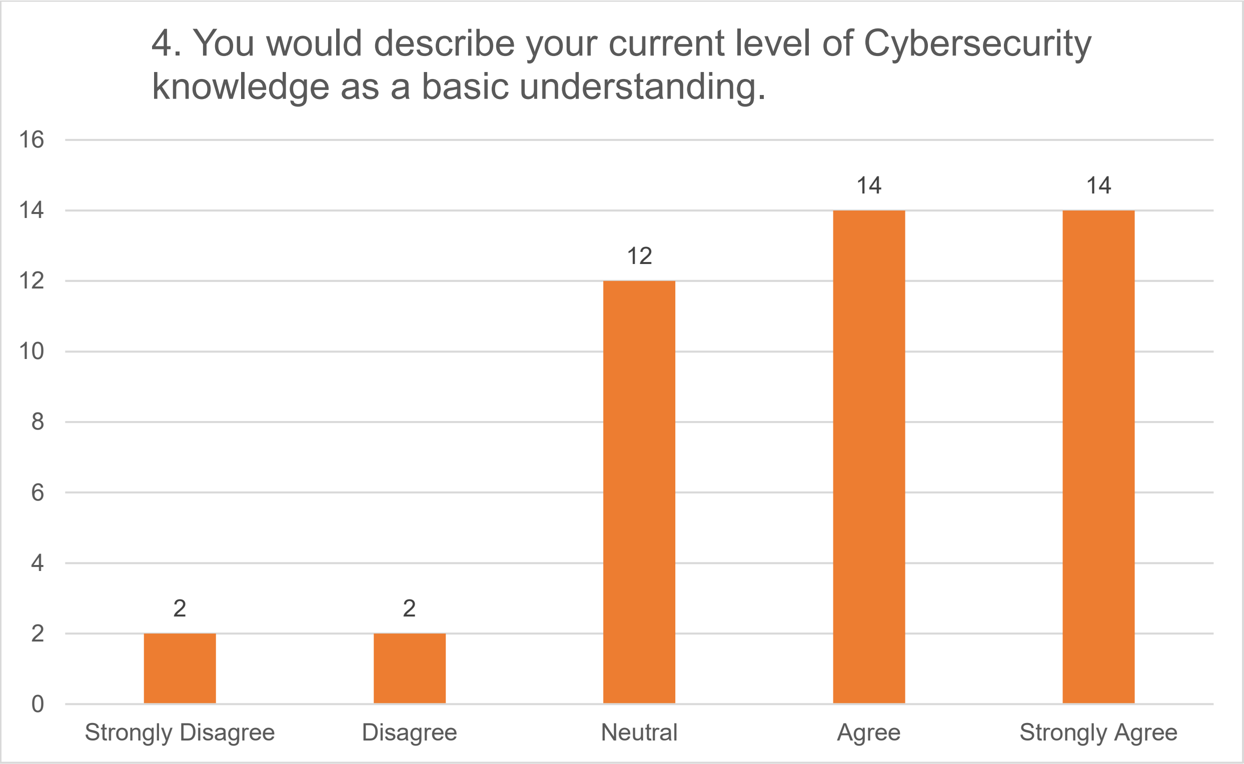
About 77% of the participants indicated that their employers provide them with cybersecurity training. Additionally, approximately 90% of the survey participants were open to pursuing cybersecurity academically or as a career option. About the same percentage were interested in pursuing cybersecurity for critical infrastructure. Finally, 84% of the survey participants were comfortable with online cybersecurity training.

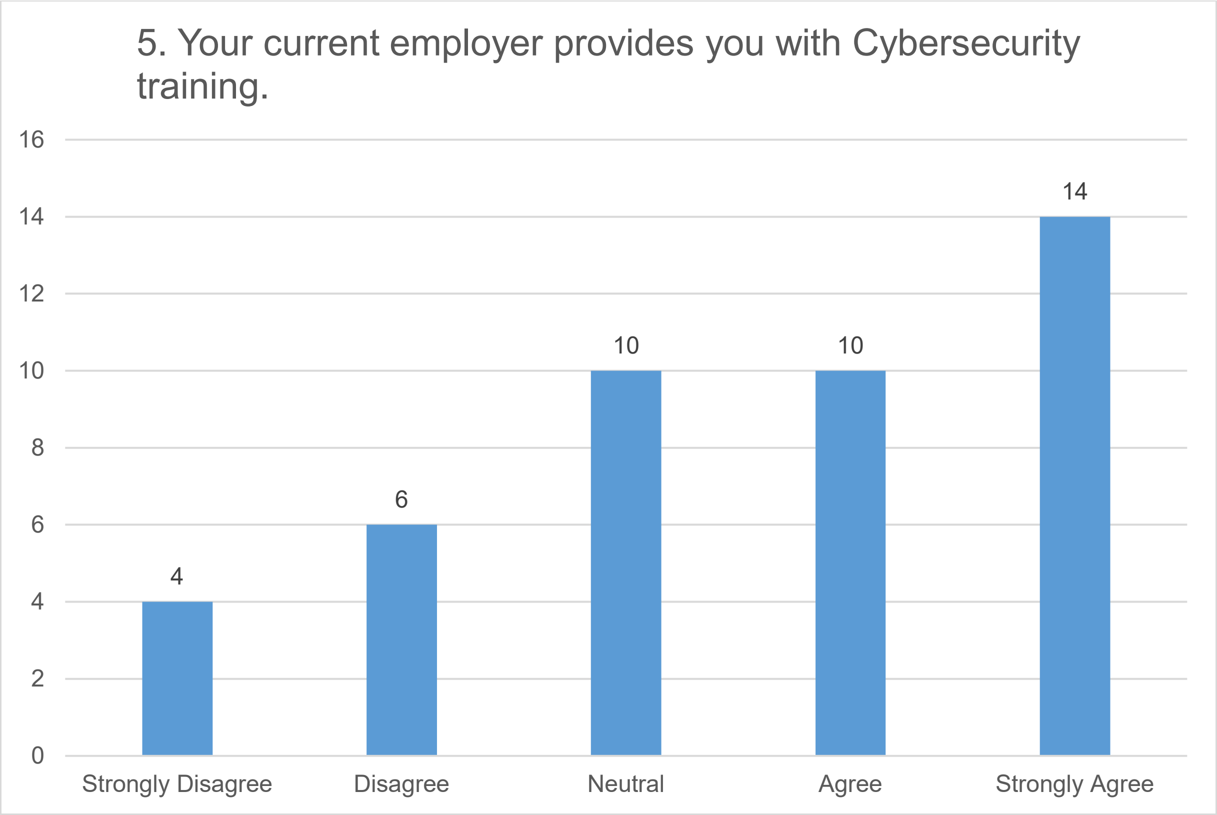
APPENDIX

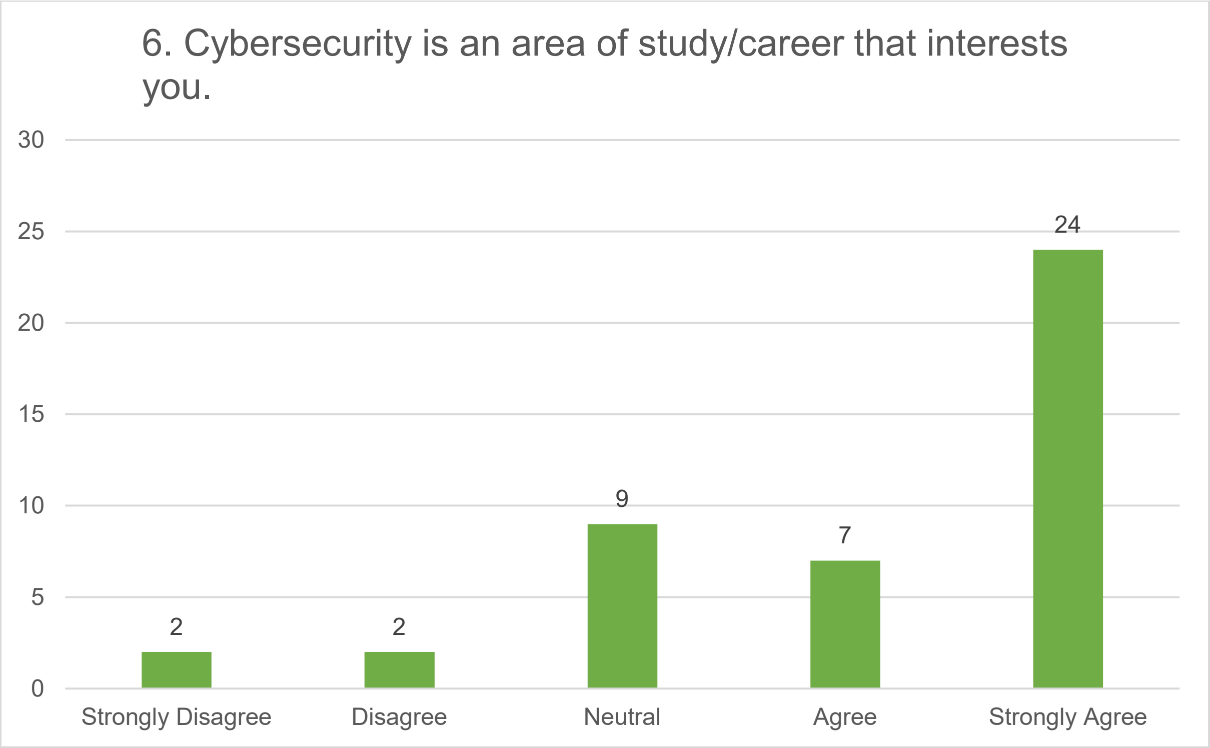

1. Which best describes your current position:
Clinical Placement Coordinator
Research Associate
Analyst
Post-Doc
Law Enfmnt
Mgmt
UMRF Mktg Admin
Elect. Engr.
Finance
Other
IT Professional
Student
Staff Member
Teacher
0
2
4
6
8
10
12
14

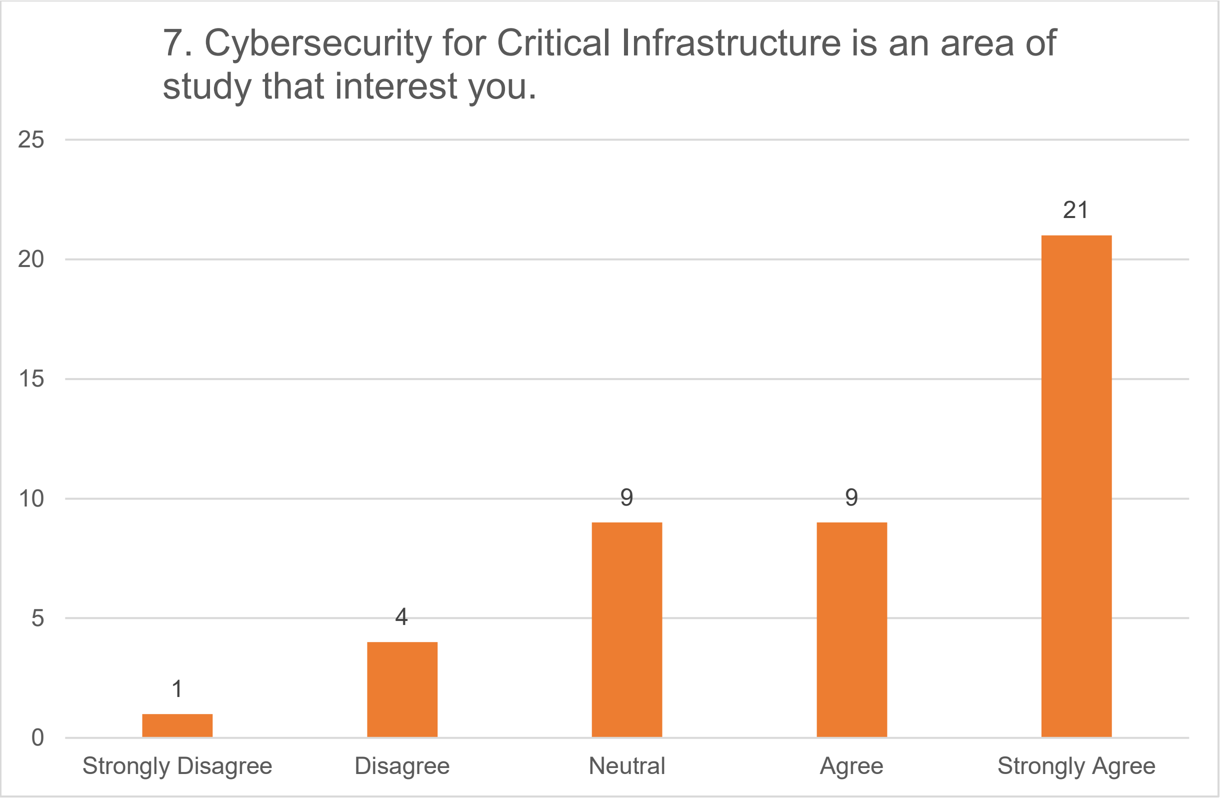

2. You would describe your current level of knowledge of Cybersecurity for Critical Infrastructure as a basic understanding.
16
14
12
10
8
6
4
2
0
3
6
12
14
9
Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree


3. Your current job responsibilities require you to understand Cybersecurity for Critical Infrastructure.
14
12
10
8
6
4
2
0
1
8
11
11
13
Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree

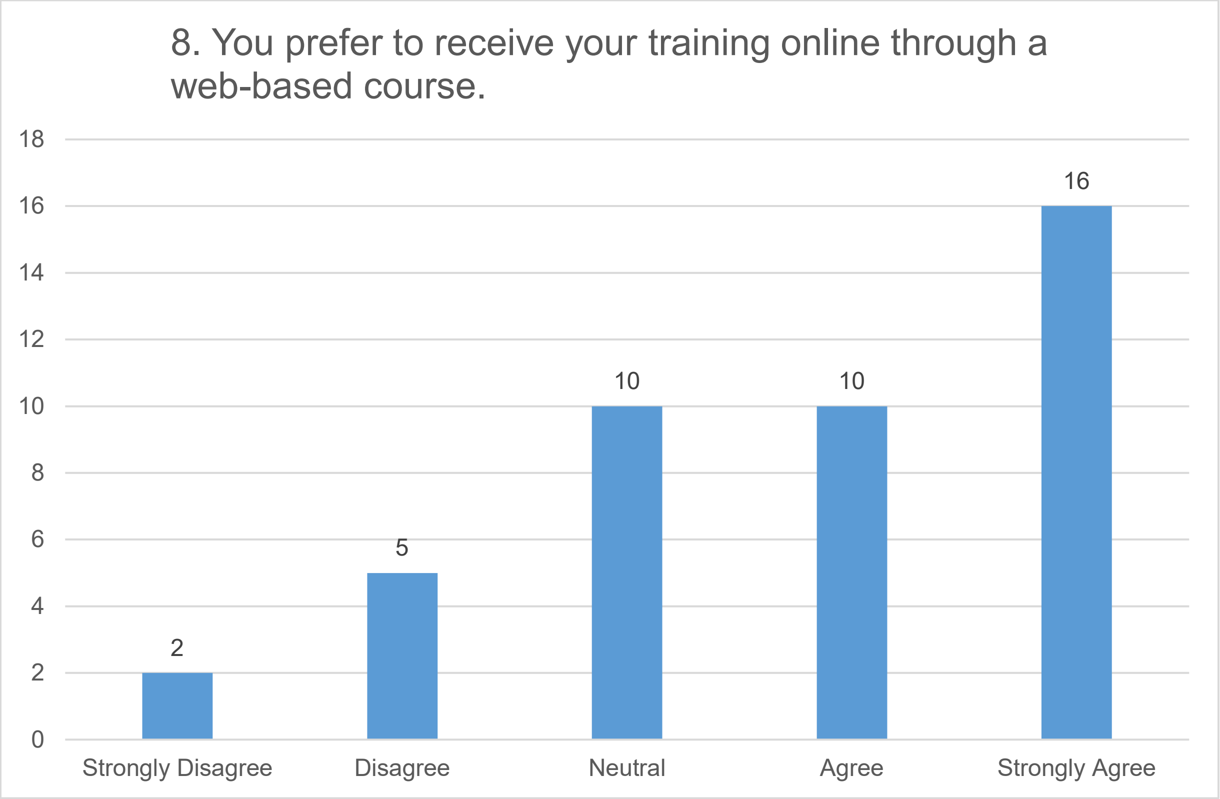

4. You would describe your current level of Cybersecurity knowledge as a basic understanding.
16
14
12
10
8
6
4
2
0
2
2
12
14
14
Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree


5. Your current employer provides you with Cybersecurity training.
16
14
12
10
8
6
4
2
0
4
6
10
10
14
Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree


6. Cybersecurity is an area of study/career that interests you.
30
25
20
15
10
5
0
2
2
9
7
24
Strongly Disagree
Disagree
Neutral
Agree
Strongly Agree



7. Cybersecurity for Critical Infrastructure is an area of study that interest you.



8. You prefer to receive your training online through a web-based course.