2023 - PDR - **CE4-1A2** - Cyber Resilience Adaptive Virtual Reality Experiences (CRAVRE) - lobof@purdue.edu - Flavio Lobo

CERIAS

The Center for Education and Research in Information Assurance and Security

Cyber Resilience Adaptive Virtual Reality Experiences (CRAVRE)

Purdue University and the Texas A&M Engineering Extension Service (TEEX) created an innovative virtual reality (VR)-based training program to help public safety officials understand the connectivity created by the Internet of Things (IoT) technologies and increase awareness around the impacts of cyberattacks on IoT for incident response and recovery during disasters.

ABSTRACT

As the IoT technologies continue to permeate communities of all sizes, the nation's cyber and cyber-physical assets are vulnerable in proportion to the increase in connectedness. Critical infrastructures, including the national power grid, health care systems, transportation systems, are highly vulnerable to cyberattacks [1,2]. So are the technologies that make cities SMART. As one author stated, "…the Internet of Things (IoT), the technology underpinning these complex and interconnected urban networks, offers a considerably expanded attack surface for cyber adversaries of all kind…"[3]. Researchers agree that the human factor plays a crucial role in preventing and limiting the impact of a cyber incident. Recent reports from various cybersecurity and data analysis firms[4,5] clearly show that human error causes up to 90% of the data breaches for corporations. Despite this, more than 40% of employees do not get regular cybersecurity training[6]. This lack of training and the resulting inadequate awareness of the connectedness is an *individual gap* that we aim to lessen. Even more startling, cybersecurity experts agree there has been an exponential increase in cybercrime during the ongoing COVID-19 crisis. While government agencies and the private sector have implemented available security frameworks[7,8], an organizational gap exists as many state, local, and critical private sector organizations continue to face deficiencies in their ability to prevent cyberattacks on their IoT technologies.

WHO IS CRAVRE FOR?

CRAVRE is designed for decision-makers at the state, tribal, and local levels of government, public safety leaders (e.g., fire, EMS, law enforcement, hospital and healthcare, public health, emergency management, etc.), key private sector stakeholders and partners, and non-governmental organizations (NGOs) who play essential roles in disaster planning, response, and recovery.

PROJECT TIMELINE & FUNDING

- Project Period: 09/2020 – 08/2023
- Funding Agency: The U.S. Department of Homeland Security
- Project Amount: $1,500,000
- More Information at https://polytechnic.purdue.edu/cravre

TEAM MEMBERS

Graduate Research Assistants

- Flavio Lobo, Miloš Stanković, Mututhanthrige Fernando

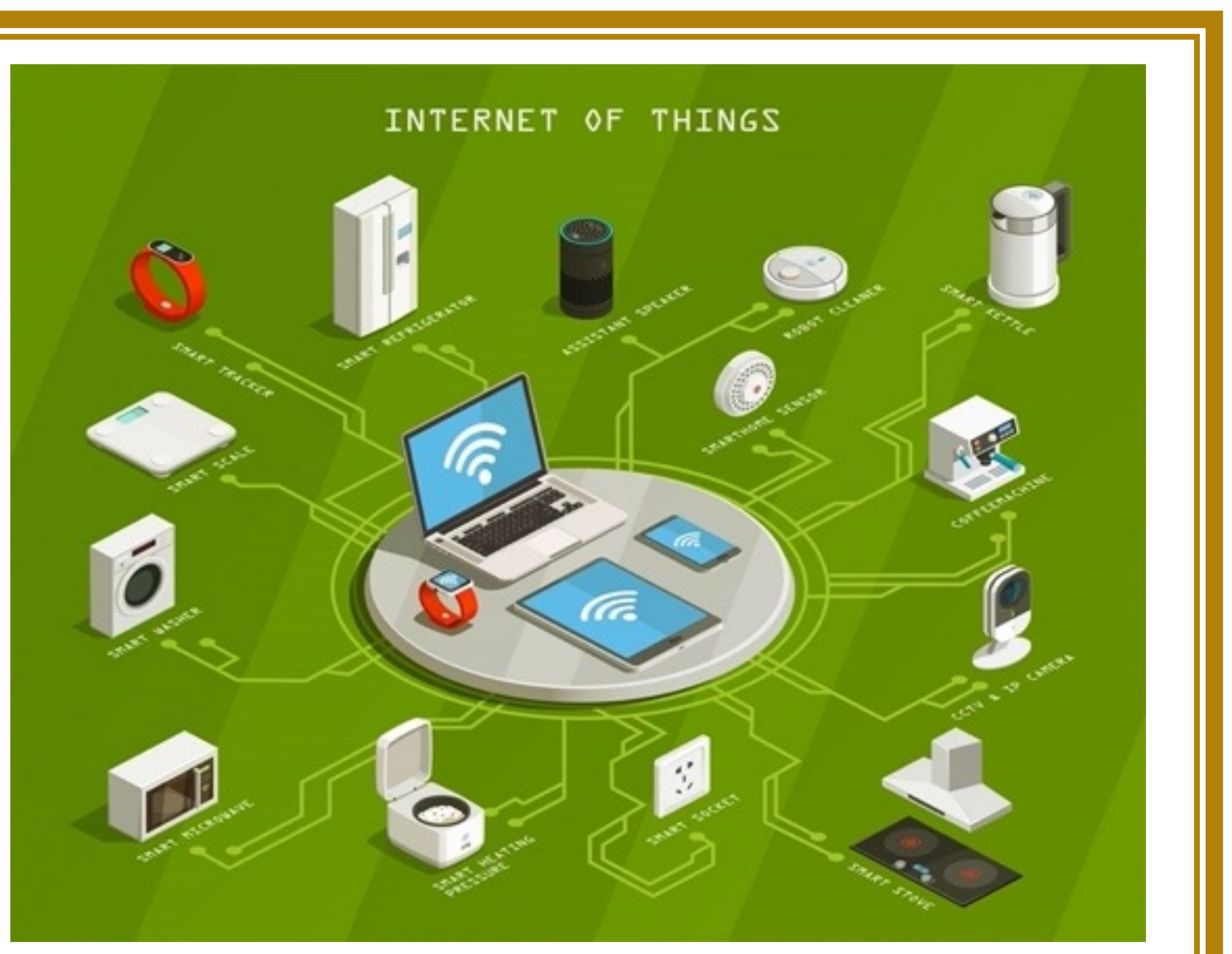
Faculty

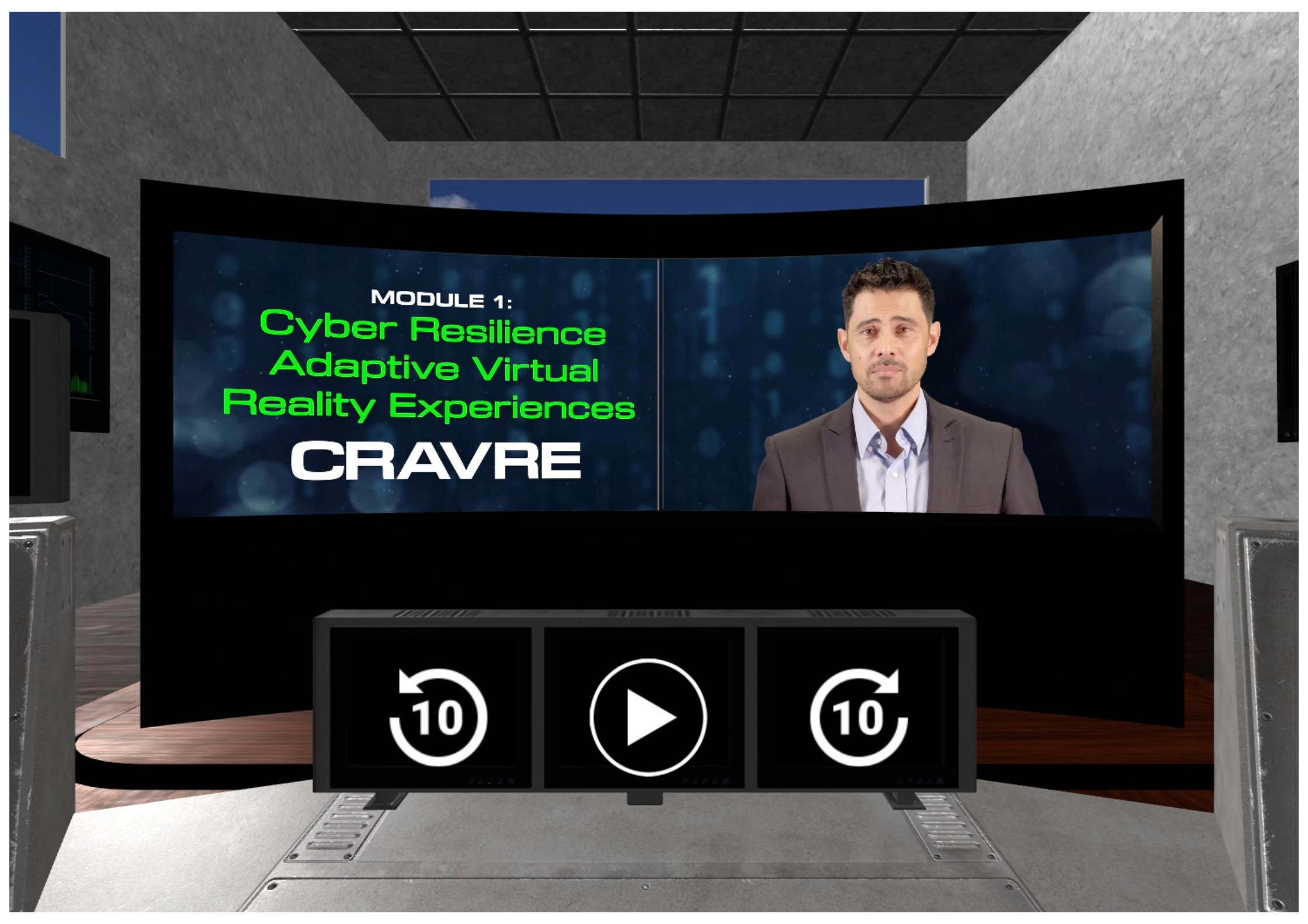
- Dr. Mesut Akdere, Dr. Umit Karabiyik, Dr. Jin Kocsis, Dr. Jason Moats

This material is based upon work supported by the U.S. Department of Homeland Security under Grant EMW-2020-CA-00061-S01.

WHY CRAVRE?

As Internet of Things (IoT) technologies continue to permeate communities, emergency planning and response organizations struggle to mitigate the increasing vulnerabilities created by the ubiquity of these technologies. CRAVRE focuses on developing strategies to detect, identify, manage, and potentially mitigate a cyber-attack as it occurs in the midst of a concurrent incident (e.g. natural disaster, terrorist attack, etc). The course addresses incident management skills, staff responsibilities, and the related situational awareness skills needed in such situations.



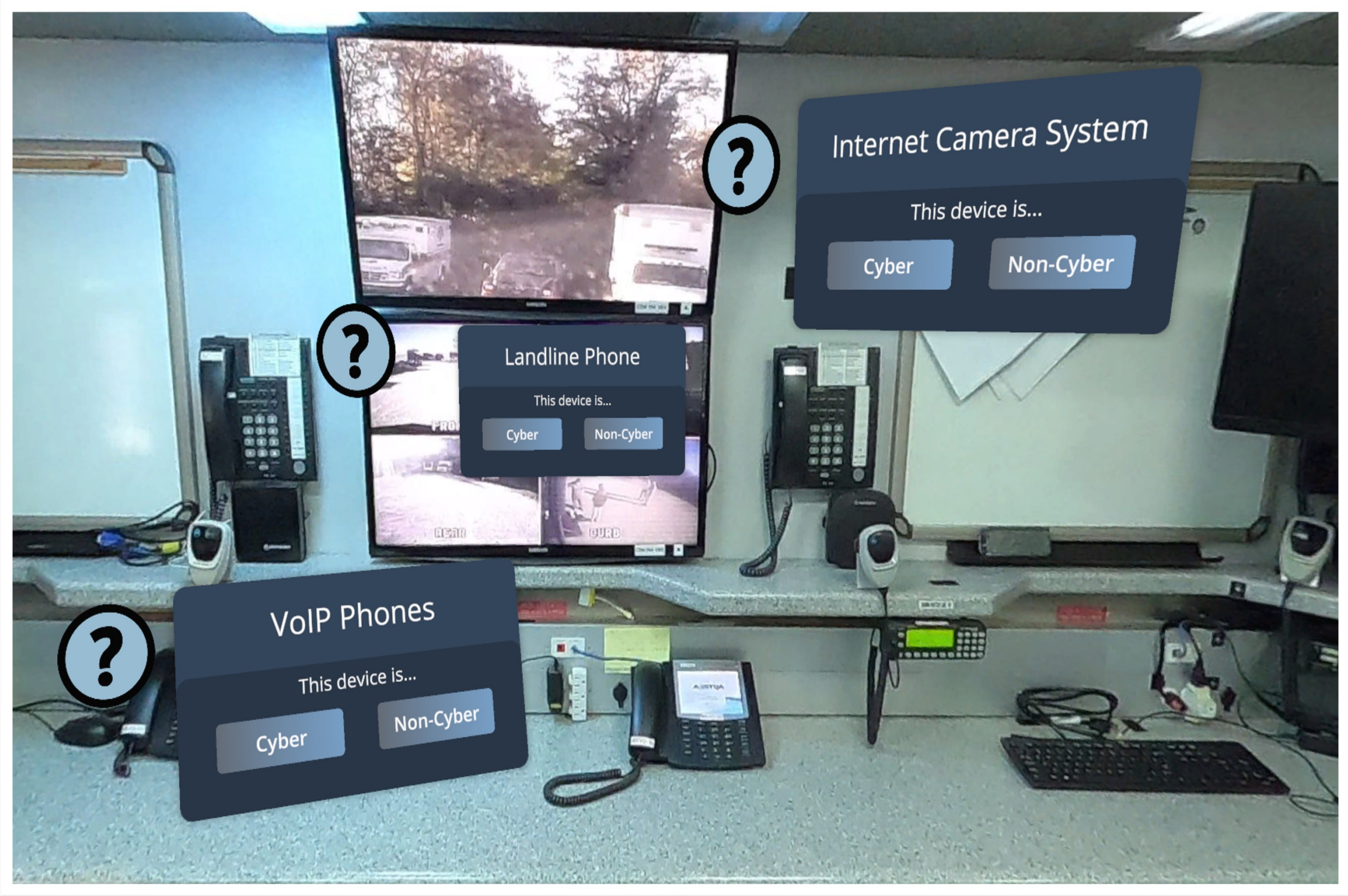


COURSE STRATEGY AND WHAT TO EXPECT

The training program is accessible through a web-based platform tailored to operate on individuals' personal devices. The training is composed of a series of scenario-based, immersive, experiential learning modules in which cyber incidents and attacks occur concurrently with natural and man-made disasters. Through these scenarios, participants will observe cause-and-effect reactions to the ubiquitous connected IoT technologies and identify strategies and techniques to adapt and prevent IoT-based attacks. Upon completing all modules, a certificate of participation is issued for the individual participants.

HOW DOES CRAVRE WORK?

CRAVRE uses scenario-based, virtual reality immersive experiences to call awareness to the complexities and vulnerabilities of the connected work of the IoT technologies. This web-based course presents participants with a challenging and adaptive environment, utilizing AI-powered personalized learning to optimally meet the cybersecurity training needs of individuals and their organizations. The training is designed to interface with a diverse selection of devices, including mobile SMART phones, tablets, laptop and desktop computers, and virtual reality headsets.



COURSE OBJECTIVES

- Students will be able to identify and interpret widely available known vulnerabilities in IoT, Critical Infrastructures (CI), Supervisory Control and Data Acquisition Systems (SCADA) as well as potential vulnerabilities during the face of natural disasters such as pandemics.*
- Students will be able to demonstrate knowledge, skills, and abilities to protect the aforementioned systems, information, and services from unauthorized access, adversarial impacts, and exploitation.*
- Students will be able to apply laws, guidelines, and digital forensics best practices pertinent to public (law enforcement) and private sector (corporate) investigations after any incidents occur.*

**Related to FEMA's Response and Recovery mission areas.*

LITERATURE CITED

(1) L. Stanaland, R. Baldick, A. A. Cardenas, and J. Holmes, "Protecting the Texas Electric Grid: A Cybersecurity Strategy for ERCOT and the PUCT," in *2019 Resilience Week (RWS)*, Nov. 2019, vol. 1, pp. 219–225, doi: 10.1109/RWS47064.2019.8972002.

(2) H. I. Kure and S. Islam, "Assets focus risk management framework for critical infrastructure cybersecurity risk management," *IET Cyber-Phys. Syst. Theory Appl.*, vol. 4, no. 4, pp. 332–340, 2019, doi: 10.1049/iet-cps.2018.5079.

(3) Digital14, "Digital14 Report: Smart Cities Unlock Business Potential but Are Increasingly Vulnerable." https://www.prnewswire.com/ae/news-releases/digital14-report-smart-cities-unlock-business-potential-but-are-increasingly-vulnerable-818572518.html (accessed Jul. 09, 2020).

(4) M. Hill, "90% of UK Data Breaches Due to Human Error in 2019," *Infosecurity Magazine*, Feb. 06, 2020. https://www.infosecurity-magazine.com:443/news/90-data-breaches-human-error/ (accessed Jul. 01, 2020).

(5) A. S. May 08 and 2019, "90 percent of data breaches are caused by human error," *TechRadar*. https://www.techradar.com/news/90-percent-of-data-breaches-are-caused-by-human-error (accessed Jul. 01, 2020).

(6) M. G. I. T. Trends 1, "43% of Employees Lack Regular Cyber Security Training," *Small Business Trends*, Oct. 10, 2019. https://smallbiztrends.com/2019/10/employee-vulnerabilities-cybersecurity.html (accessed Jul. 09, 2020).

(7) M. P. Barrett, "Framework for Improving Critical Infrastructure Cybersecurity Version 1.1," Apr. 2018, Accessed: Jul. 01, 2020. [Online]. Available: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11.

(8) nicole.keller@nist.gov, "Cybersecurity Framework," *NIST*, Nov. 12, 2013. https://www.nist.gov/cyberframework (accessed Jul. 01, 2020).