Cyber Resilience Adaptive Virtual Reality Experiences (CRAVRE) is an innovative training approach made to increase awareness of the vulnerabilities created by the Internet of Things (IoT) technologies among public safety officials and the impact of cyberattacks on incident response and recovery.

CRAVRE encompasses a Whole Community approach that addresses preventing the IoT-based attacks for Emerging Threats: Cybersecurity.

Increasing Cybersecurity Threats

Researchers agree that the human factor plays a crucial role in preventing and limiting the impact of a cyber incident, even when the security of other categories is satisfied. Recent reports from various cybersecurity and data analysis firms 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.

Cybersecurity experts agree that 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, 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.

Immersive Virtual Reality Modules

CRAVRE offers scenario-based, immersive, experiential learning opportunities in which cyber incidents occur concurrently with another disaster. Through these scenarios, participants observe cause-and-effect reactions to the ubiquitous connected IoT technologies and identify strategies and techniques to adapt and prevent IoT-based attacks.

Al-powered Learner-in-the-Loop Personalized Learning Module

- Adaptive granularity meets the needs of both the individual and the prescribed outcomes of the training
- Secure and privacy-preserving data acquisition and storage system captures and integrates the offline data from the learners, including learner demographics, prior learning experiences, and performance data, self-expressed learning preferences, and course evaluations
- The data fusion mechanism:
  - Synthesizes the multimodal, multivariate, and multitemporal data for the individual learners
  - Analyzes the data to automatically recognize the individual learning features
  - Implements data-driven online decision makings on identifying and forecasting both learning and instruction gaps
- Fills in the gaps on an individual basis by adapting the learning plan and providing tailored-support and guidance

REFERENCES

1. “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 kinds...”
2. DigitalCit, SmartCities, The future, the trend, the Application
9. FEMA’s Response and Recovery mission areas).