U.S. DEPARTMENT OF ENERGY | Office of Cybersecurity, Energy Security, and Emergency Response

Assessing Perceptions and Culture of Cybersecurity Within an Organization

CREDC
CYBER RESILIENT ENERGY DELIVERY CONSORTIUM

Assessing human perception of cybersecurity to increase the effectiveness of training and resource allocation

It is difficult for human system operators to consider "concrete" aspects of cybersecurity, such as the number of known attempted attacks and mean-time-to-failure, when reacting to security concerns in real time. Cybersecurity decisions are instead driven by "non-concrete" attitudes and perceptions of security. It is important to understand an organization's culture of cybersecurity in order to mitigate these internal decision-making issues. Most organizations are becoming increasingly concerned about cybersecurity, but often do not have a scientifically grounded basis for determining what they should do. The results of this project enable the assessment and comparison of cybersecurity cultures across organizations and how they change. This will help organizations determine where to devote additional attention and resources and evaluate the effectiveness of these efforts over time.

KEY TAKEAWAYS

- Assesses attitudes pertaining to cybersecurity based on a statistically validated 7-point scale
- Enables organizations to identify necessary adjustments to training and resource allocation based on employee attitudes and perceptions of security
- Recognizes variations in perceptions based on different industries, levels of an organization, or functions

OUTCOME

This research equips energy delivery system operators with metrics to understand the effectiveness of their cybersecurity training programs. Standardized measures support regular self-assessment and allows operators to determine necessary program adjustments or funding reallocation.

PARTICIPANTS	ROLE
CREDC CYBER RESILIENT ENERGY DELIVERY CONSORTIUM	The CREDC performs multidisciplinary research and development that focuses on the cybersecurity of energy delivery systems. The central project goal is to create an ecosystem where research results lead directly to the development of applications and methodologies, which are then validated in realistic contexts.
Massachusetts Institute of Technology	Leads research, development, and testing

CONTACT INFORMATION

Initial Leads:

Carol Hawk
Program Manager

Stuart Madnick
Site Lead, Professor
Massachusetts Institute of Technology
617-253-6671
smadnick@mit.edu

Current Contact as of February 2020:

Akhlesh Kaushiva
Senior Technical Systems and Cybersecurity Advisor
Department of Energy (DOE)
Office of Cybersecurity, Energy Security, and Emergency Response (CESER)
202-287-6062
Akhlesh.Kaushiva@hq.doe.gov

This is a subproject sponsored by the CREDC academic consortium, led by the University of Illinois.

CREDC Period of Performance: October 2015 – May 2022

CREDC Total Award Value: $28,099,258
DOE Share: $22,476,290
Cost Share: $5,622,968

CYBERSECURITY FOR ENERGY DELIVERY SYSTEMS (CEDS)

CEDS projects are funded through DOE CESER, which aims to enhance the reliability and resilience of the nation's energy infrastructure by reducing the risk of energy disruptions due to cyberattacks.

Website: https://www.energy.gov/ceser

Date Written: June 2021