

NICE FRAMEWORK SUCCESS STORY

Social Engineering Competitions
The CARE Lab, Temple University

Cybersecurity Education and Evaluation

The voluntary [Workforce Framework for Cybersecurity](#) (NICE Framework) was developed through a collaborative process by industry, academia, and government stakeholders. It establishes a taxonomy and common lexicon that describes cybersecurity work and is intended for use in both the public and private sectors. NIST does not validate or endorse any individual organization or its approach to using the NICE Framework.

ORGANIZATIONAL PROFILE

Cyberspace is fundamental to our national prosperity, as it is critical to economy, government, and day-to-day societal functioning. The Cybersecurity in Application, Research, and Education (CARE) Lab offers a social science approach to cybersecurity and seeks to foster a multidisciplinary dialog between academia, industry, nonprofits, and government. This intersectionality enables a creative, unique, and holistic means of understanding the phenomena of cyberattacks and cybersecurity. Additionally, the CARE Lab offers free course projects and datasets for download that can be (and have been) used by students, educators, and industry and government representatives across multiple sectors. Our research and education projects have been funded by several National Science Foundation grants. The CARE Lab is committed to diversity, equity, and inclusion (DEI) efforts and embraces the "cybersecurity is for everyone" mindset.

WHY WE USE THE NICE FRAMEWORK

The NICE Framework offers a consistent and well-recognized taxonomy. The statements that serve as the building blocks of the framework help the CARE Lab effectively communicate the relevance of social engineering (SE) to academia, industry, and government.

PROJECT DRIVERS

The CARE Lab aimed to emphasize the relevance of the human behavior and socio-psychological factors in cyberattacks. We determined that the most effective way to do so would be via competitions that highlight scenarios that emulate how cybercriminals are increasingly leveraging SE in their attacks. We turned to the NICE Framework to serve

as a foundation for these efforts, in support of the following goals:

- To develop a strong academic-industry-government-nonprofit nexus that brings in realistic and different cybersecurity perspectives to enhance student learning experiences.
- To promote DEI by making our SE competitions accessible to students from underrepresented communities and provide a safe, ethical, cost-effective, and fun learning experience.
- To promote a non-technical way of thinking about cyberattacks and cybersecurity that is inclusive of all disciplines, skills, and education levels.

"Since the 'human factor', ultimately, is the root cause of most security breaches within an organization, we are fascinated with what we believe is an ever-evolving area of the cybersecurity world. We hope to further explore the connections between ... psychology ... and the impact it has ... on cybersecurity"

2021 Social Engineering Event
Competing Team

PROCESS

1. The CARE Lab conducted an initial mapping of various classroom SE projects to the NICE Framework Knowledge, Skill, and Ability (KSA) statements.

2. The course project mapping process was reviewed and fine-tuned over the course of several semesters to ensure consistent mapping.
3. The refined mapping process was then scaled up to apply to two (inter)national SE competitions: the Summer Social Engineering Event and the Collegiate Social Engineering Capture-the-Flag (SECTF) competition. The mapping process informed the competitions' design, components, and structure.
4. Finally, the CARE Lab created a feedback loop where competition participants are surveyed about the various KSA components to understand whether these are truly being captured in the competitions.

BENEFITS & IMPACT

- The detailed taxonomy of roles and KSAs of the NICE Framework have allowed the CARE Lab to bring SE into mainstream cybersecurity education conversations.
- The NICE Framework has helped the CARE Lab solidify its message to non-technical students that not all cybersecurity careers require technological skills; having a different (non-technical) disciplinary background is a strength and not a weakness.
- The NICE Framework has helped the CARE Lab develop pre- and post-competition surveys that provide metrics on student learning specific to KSAs.



Figure 1: Winners of the 2021 Social Engineering Pen Testing Competition

CONTACT INFORMATION & RESOURCES

Contact:

- ▶ Anshul Rege, Director of the CARE Lab
rege@temple.edu

Websites:

- ▶ sites.temple.edu/care
- ▶ sites.temple.edu/socialengineering
- ▶ sites.temple.edu/collegiatesectf

January 2022