Building and evidencing competencies in the cybersecurity classroom

Dr. Vincent Nestler

Dr. Zoe Fowler

Tuesday September 19 2023, NCEC

CALIFORNIA STATE UNIVERSITY SAN BERNARDINO

NORWICH UNIVERSITY

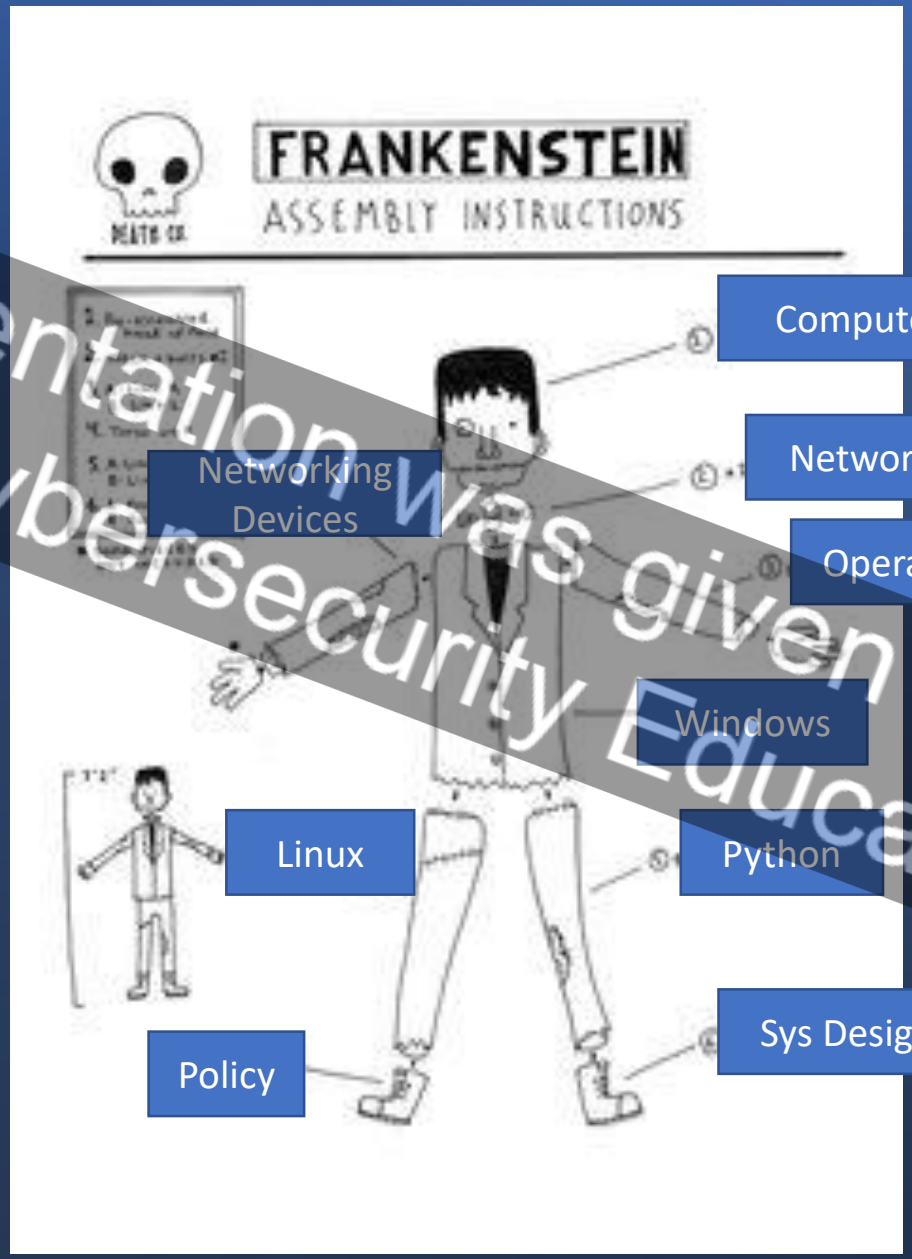
Careers Preparation National Center

Overview of session

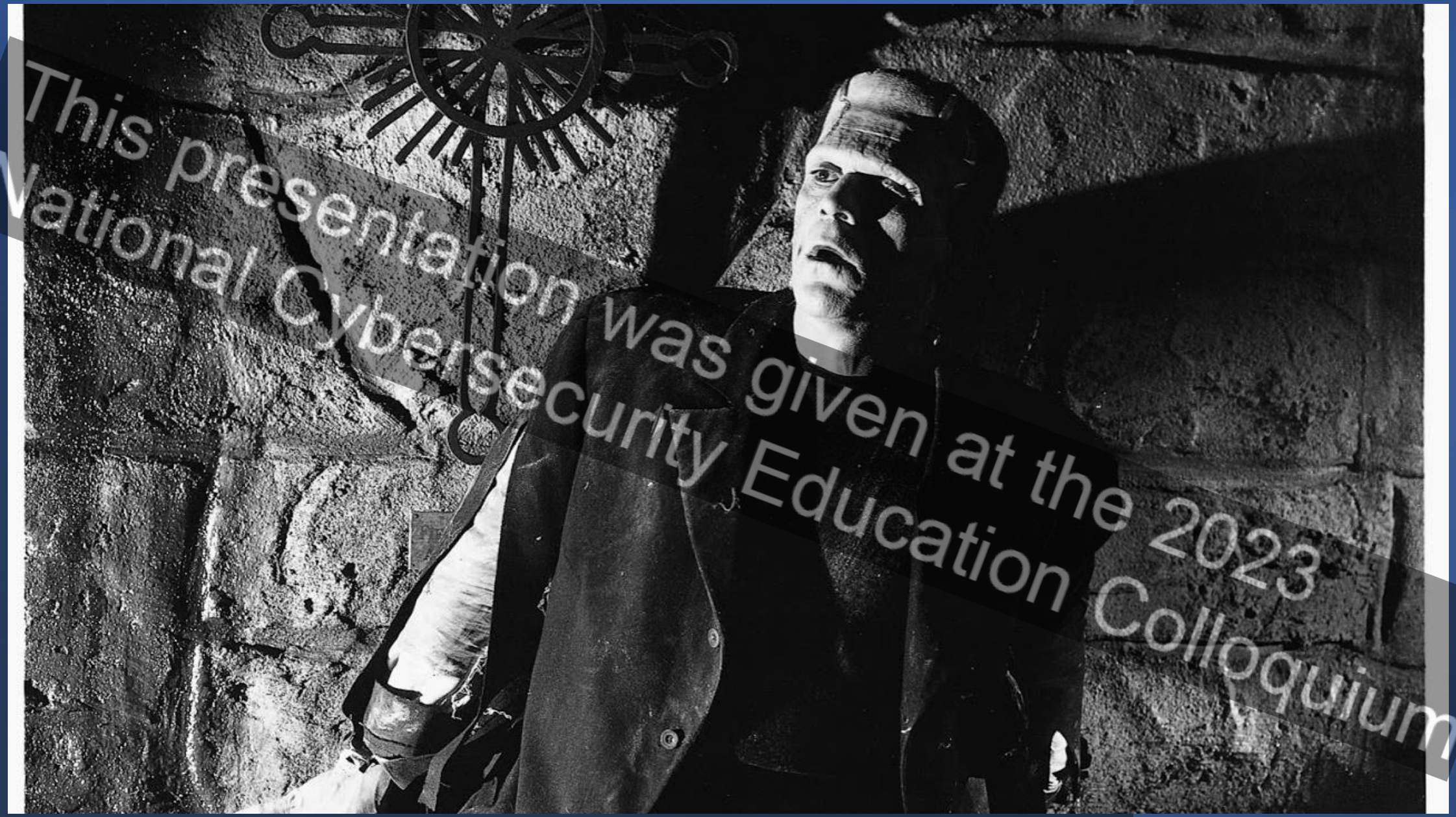
- The problem: Frankenstein's monster
- Step 1: start with the work role
- Step 2: learning your ABCDEs
- Step 3: Inputs and outputs
- Spreading the word

Educating Frankenstein's Monster

- Computer Skills
- Networking Skills
- Operating Systems
- Network Devices
- Windows
- Linux
- Coding and Scripting
- Etc.

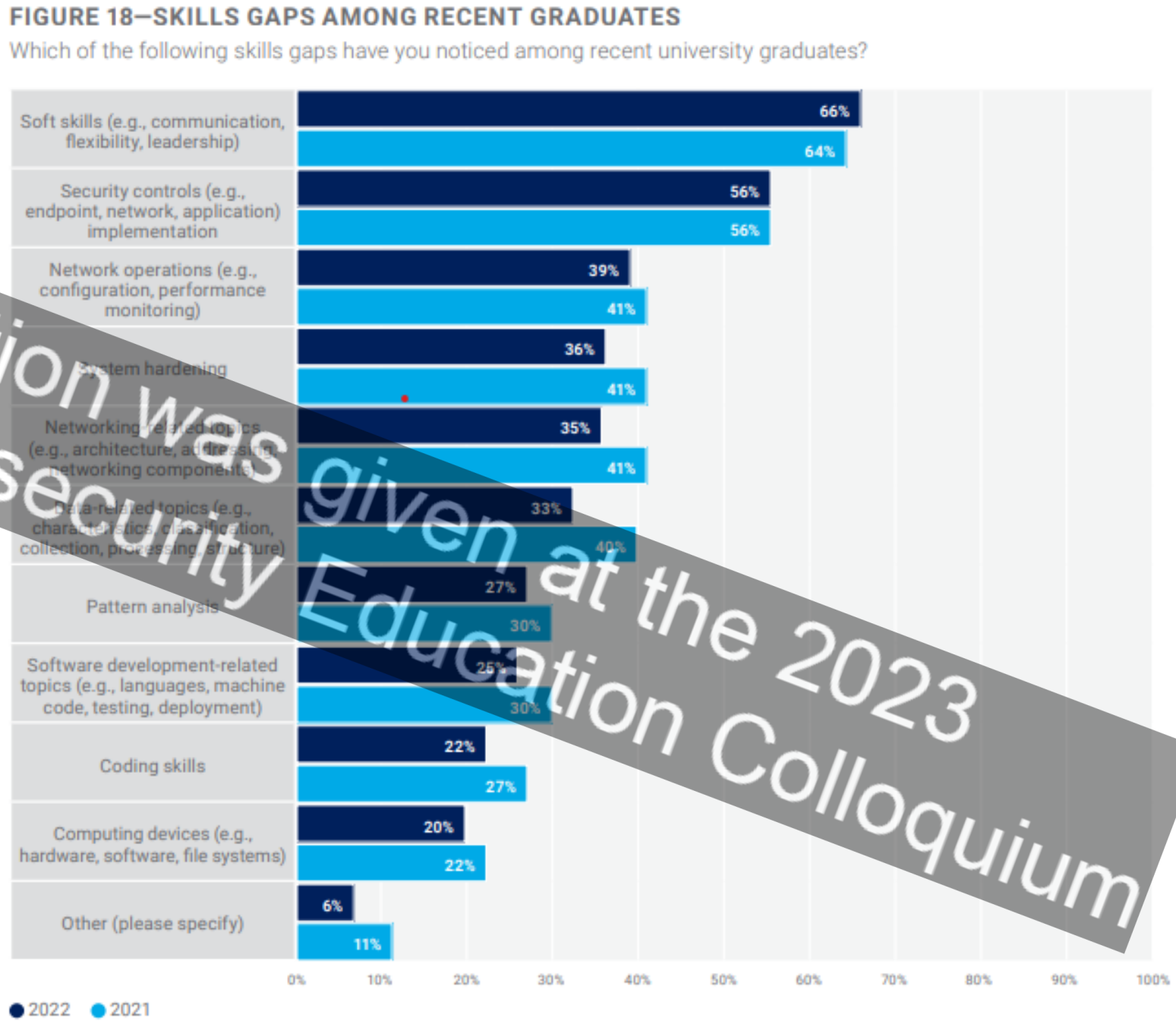



This presentation was given at the 2023
National Cybersecurity Education Colloquium


This presentation was given at the 2023
National Cybersecurity Education Colloquium

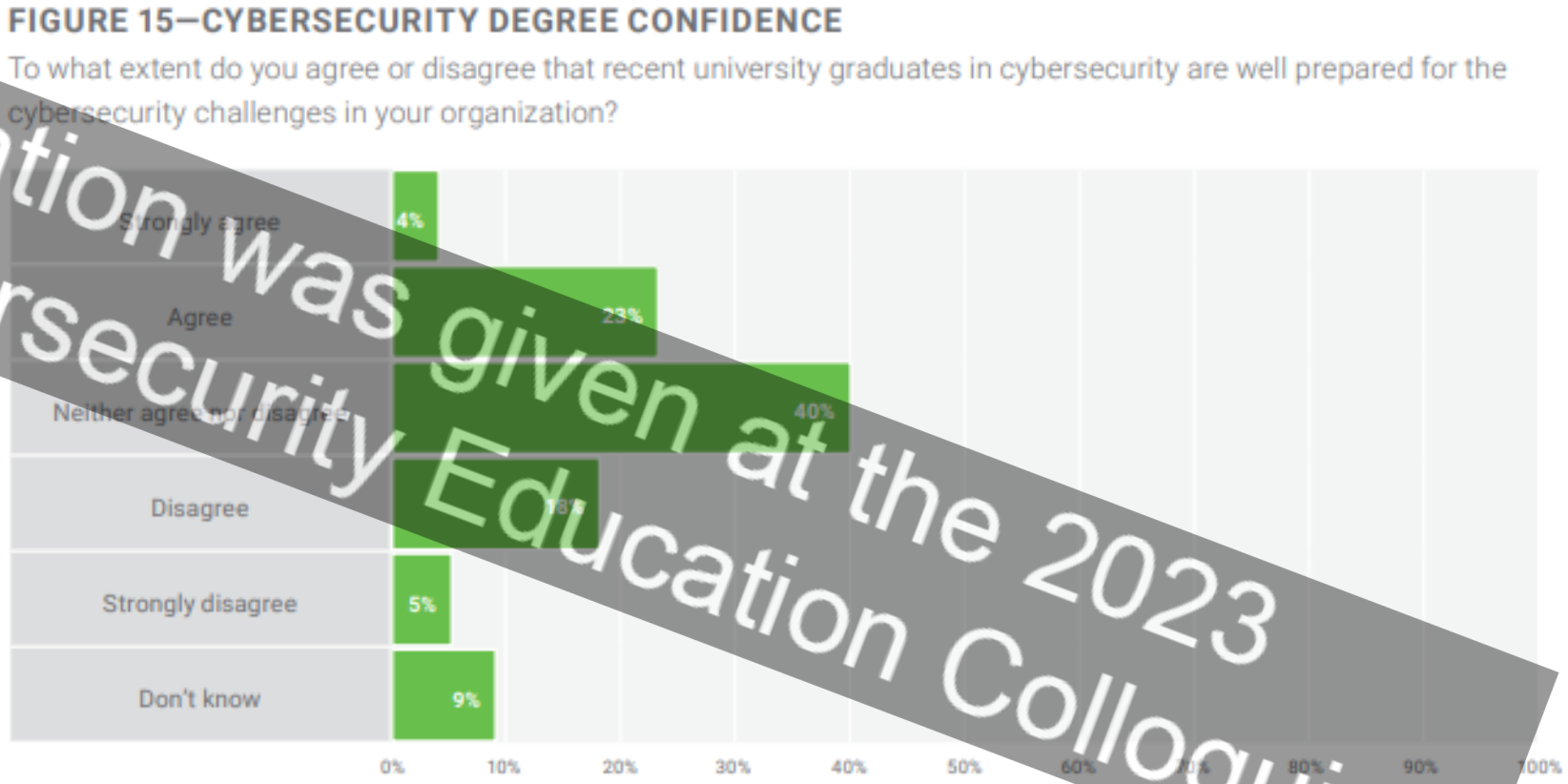
The Skills Gap Stats

From ISACA - State of Cyber Security 2022



The Skills Gap Stats

From ISACA - State of Cyber Security 2022



Reasons for this disconnect pt.1

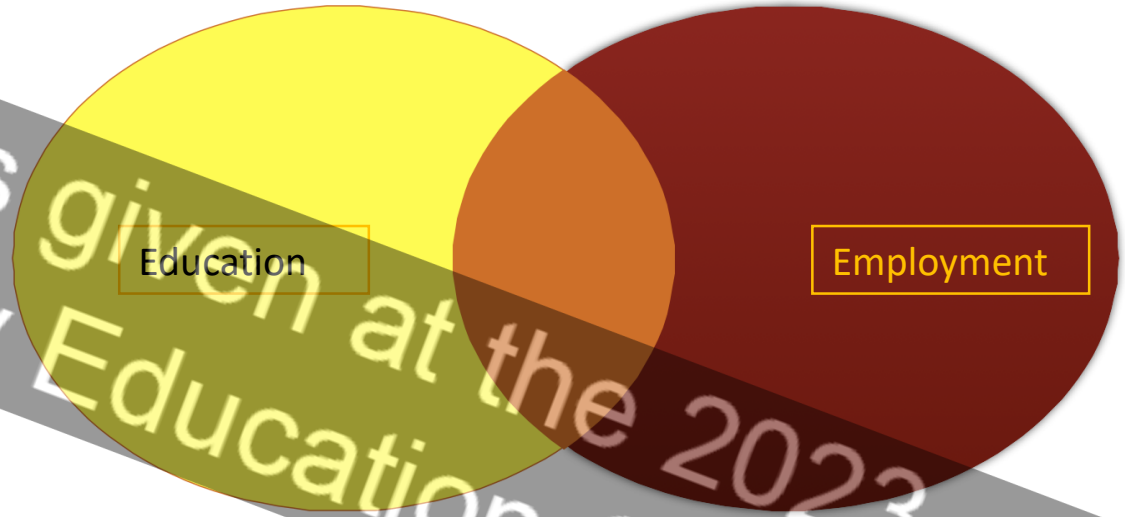
- Challenge of providing a contextualized learning experience both in terms of a realistic work environment with realistic tasks to be accomplished.
- Students graduate with component skills but without opportunities to engage in simulated work environments.
- Because many skills are taught in isolation of other skills (Linux, Windows, networking devices, coding, etc) those skills may be lost and forgotten by the time of graduation.

Reasons for this disconnect pt.2

- We start too late.
- Lack of hands-on experience opportunities
- Students lack knowledge of available work roles, and therefore lack self-efficacy in designing careers which they will enjoy and where they will excel.

Talking about competency

- Transforms knowledge and skills into workplace capabilities.
- Develops "breach-ready" workforce.
- Potential win-win-win situation (win for the educator, win for the employer and, most importantly, win for the student)
- BUT, important that we are all speaking the same language



“COMPETENCY IS
THE ABILITY FOR THE STUDENT
TO COMPLETE A TASK OR TASKS
WITHIN THE CONTEXT OF A WORK ROLE.”

Step 1:

Begin with the work role

DoD Cyber Workforce Framework

The DoD Cyber Workforce Framework establishes the DoD's authoritative lexicon based on the work an individual is performing, not their position titles, occupational series, or designator.The DCWF describes the work performed by the full spectrum of the cyber workforce as defined in DoD Directive (DoDD) 8140.01. The DCWF leverages the original National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework (NCWF) and the DoD Joint Cyberspace Training and Certification Standards (JCT&CS).

Workforce Elements

Workforce Elements | Elements Map | Search Work Roles | Search KSATs

Click the arrow to expand/collapse the Workforce Elements. Then select the Workforce Element to see the associated Work Roles.

IT Cyberspace

IT (Cyberspace)

Personnel who design, build, configure, operate, and maintain IT, networks, and capabilities. This includes actions to prioritize implement, evaluate, and dispose of IT as well as information resource management; and the management, storage, transmission, and display of data and information.

Workforce Framework for Cybersecurity (NICE Framework)

Categories/Specialty Areas | Work Roles | Tasks | Knowledges | Skills | Abilities

The Workforce Framework for Cybersecurity, commonly referred to as the NICE Framework, is a nationally focused resource to help employers develop their cybersecurity workforce. It establishes a common lexicon that describes cybersecurity work and workers regardless of where or for whom the work is performed. The NICE Framework applies across public, private, and academic sectors.

The NICE Framework is comprised of the following components:

- Categories (7) – A high-level grouping of common cybersecurity functions
- Specialty Areas (33) – Distinct areas of cybersecurity work
- Work Roles (52) – The most detailed groupings of cybersecurity work comprised of specific knowledge, skills, and abilities (KSAs) required to perform tasks in a Work Role

To explore the NICE Framework, click on the Categories below or use the links above to search within the NICE Framework components or by keyword. To learn more, review the Using the NICE Framework PDF.

DISCUSSION

- Choose a work role that interests you.
- Identify educational activities suited to prepare you for these tasks?
- Think of curricular (e.g. classroom-based), co-curricular (e.g. exercises, tools) and extra-curricular (e.g. competitions, internships) that might prepare you for these tasks.

Step 2:

Build a competency statement (ABCDE)

The Essential Elements of Competency

Competency is most effectively described using 5 key elements:

A - actor (who exhibits the competency);

B - behavior (what task the actor is expected to complete);

C - context (how the behavior is enacted);

D - degree (how much time, accuracy and degree of completion);

E - employability (what professional skills are necessary for this task to be enacted in a way that would be appropriate for the workplace).

A - actor (who exhibits the competency);

B - behavior (what task the actor is expected to complete);

C - context (how the behavior is enacted);

D - degree (how much time, accuracy and degree of completion);

E - employability (what professional skills are necessary for this task to be enacted in a way that would be appropriate for the workplace).

Cybersecurity students taking an IS136 Disaster Recovery Business Continuity level community college course who have completed Introduction to Information Systems, Information to Operating Systems and Networking Security Fundamentals will act as vulnerability assessment analysts (VAM) with access to the risk assessments of Dr. Know's medical office network and the CSET 10.3 tool to perform technical and non-technical risk and vulnerability assessments of the local computing environment (T0549). They will identify 5 key risks within 4 hours and produce a risk assessment and recommendations report which clearly communicates the found risks for a non-technical user.

A - Actor

- Identify level of participant (e.g. high schooler, freshman, junior etc.)
- State any previous courses and/or knowledge they should have acquired before attempting this competency
- Summarize assumed level of knowledge
- Infers anticipated level of proficiency

B - Behavior

- Corresponds with work role and task listed in existing frameworks (e.g. NICE framework or DoD DCWF)
- Identifies work role and specific task (s)
- Note: identifying the task and work role builds a direct connection between the educational activity and the workplace.

C - Context

- This is the context in which the task is performed.
- Describe the scenario in which the competency is demonstrated.
- What resources and technology are provided, what constraints are enforced.

D - Degree

- Identifies how much time might be assumed for competent engagement with task, how much accuracy is required and how much of the task needs to be completed
- Shifts focus from academic (potential 100% by each individual) to 'would this be good enough for an employer?'

E - Employability

- A person can be technically able but remain unemployable unless they also have the professional skills required by a specific workplace.
- Professional skills tend to include teamwork, critical thinking, communication, integrity, and ethical judgement and reasoning (https://www.montreat.edu/student-life/montreat-360/).
- These cannot be tacitly assumed, but need to be identified and stated.

Step 3:

Inputs and Outputs

CPNC

Next steps

- Workshops on Thursday 21st and Friday 22nd September (NCEC)
- Two day workshop on Thursday 12th and Friday 13th October
- E-Handbook available - https://www.caecommunity.org/national-center/careers-preparation-national-center
- Contact zfowler@norwich.edu