Pre-Bachelor's Curricular Guidance for Cybersecurity Programs

Cara Tang, Portland Community College
Melissa Stange, Lord Fairfax Community College*

Cindy Tucker,
Bluegrass Community & Technical College

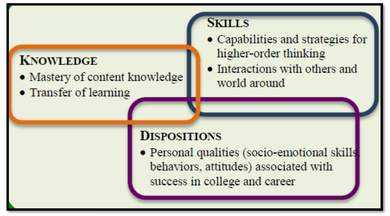
Markus Geissler, Cosumnes River College
Christian Servin, El Paso Community College

Goal

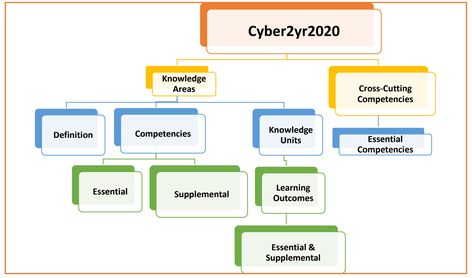
Develop curriculum guidelines for *Cybersecurity Pre-Bachelor Programs, called Cyber2yr2020* as a spin-off from CSEC2017. Map to NICE Cybersecurity Workforce Framework, ABET CAC Criteria 3 & 5 for associate programs, Center of Academic Excellence in Cyber Defense Knowledge Units and existing programs.

Focus

Competencies = Knowledge + Skills + Dispositions

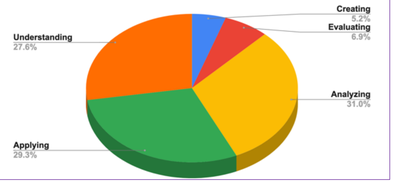


Design



Content

Bloom's Competency Distribution



Knowledge Areas / Domains & Knowledge Units / Subdomains

Data	Cryptography Digital Forensics Data Integrity and Authentication Access Control	Secure Communication Protocols Cryptanalysis Data Privacy Information Storage Security
Software	Fundamental Principles Design Implementation Analysis and Testing	Deployment and Maintenance Documentation Ethics
Component	Component Design Component Procurement	Component Testing Component Reverse Engineering
Connection	Physical Media Hardware and Physical Component Interfaces and Connectors Distributed Systems Architecture	Network Architecture Network Implementations Network Services Network Defense
System	System Thinking System Management System Access and Control	System Testing Common System Architectures
Human	Identity Management Social Engineering Personal Compliance with Cybersecurity Rules/Policy/Ethical Norms	Awareness and Understanding Personal Data Privacy and Security Usable Security and Privacy
Organizational	Risk Management Security Governance & Policy Analytical Tools Systems Administration	Cybersecurity Planning Business Continuity, Disaster Recovery, and Incident Management Security Program Management Personnel Security
Societal	Cybercrime Cyber Law Cyber Ethics	Cyber Policy Privacy

Software Security

Definition

Focuses on the development of software with security and potential vulnerabilities in mind so that it cannot be easily exploited.

The security of a system, and of the data it stores and manages, depends in large part on the security of its software. The security of software depends on how well the requirements match the needs that the software is to address, how well the software is designed, implemented, tested, and deployed and maintained. The documentation is critical for everyone to understand these considerations, and ethical considerations arise throughout the creation, deployment, use, and retirement of software.

Essential Competencies

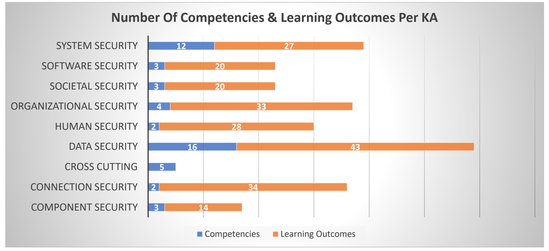
- [SOF-E1] Write secure code with appropriate documentation for a software system and its related data. *Applying*
- [SOF-E2] Analyze security and ethical considerations at each phase of the software development lifecycle. *Analyzing*
- [SOF-E3] Use documentation, such as third-party library documentation, in a given secure computing scenario. *Applying*

Supplemental Competencies

- [SOF-S1] Implement isolation to secure a process or application. *Applying*
- [SOF-S2] Discuss the relationship between an organization's mission and secure software design. *Understanding*
- [SOF-S3] Write software specifications, including security specifications, for a given process or application. *Applying*
- [SOF-S4] Assess a given test plan, from a security perspective. *Evaluating*
- [SOF-S5] Examine social and legal aspects of software development from a security perspective. *Analyzing*
- [SOF-S6] Develop user documentation for software installation with security appropriately included. *Creating*

Knowledge Units

Fundamental Principles Design Implementation Analysis and Testing	Deployment and Maintenance Documentation Ethics



Rubrics

Component Security

Emerging	Learning Outcome - Developed	Highly Developed
Component Design		
Recognize that a component's design may create vulnerabilities in information systems. *Remembering*	Discuss how a component's design may create vulnerabilities in information systems. *Understanding* [COM-LO-E01]	Illustrate how a component's design may create vulnerabilities in information systems. *Applying*
Component Procurement		
List some vulnerabilities, risks, and mitigations for components of an organizational network in a supply chain. *Remembering*	Discuss vulnerabilities, risks, and mitigations for components of an organizational network at various points in a supply chain. *Understanding* [COM-LO-E02]	Analyze vulnerabilities, risks, and mitigations for components of an organizational network at various points in a supply chain. *Analyzing*
Name some security threats and risks to hardware and software in component procurement. *Remembering*	Discuss security threats and risks to both hardware and software in component procurement, such as malware attached during manufacturing or transportation. *Understanding* [COM-LO-E03]	Outline security threats and risks to both hardware and software in component procurement. *Analyzing*

Program Examples

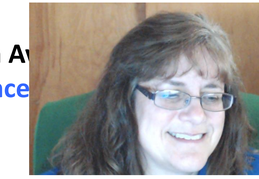
Bluegrass Community & Technical College
Ivy Tech Community College
Lord Fairfax Community College

Highlight your Cybersecurity Program: `ccecc.acm.org/correlations`

acm CCECC Committee for Computing Education in Community Colleges

SCAN ME

More Information Av
ccecc.acm.org/guidance



Pre-Bachelor's Curricular Guidance for Cybersecurity Programs

Cara Tang,
Portland Community College

Melissa Stange,
Lord Fairfax Community College

Cindy Tucker,
Bluegrass Community & Technical College

Markus Geissler,
Cosumnes River College

Christian Servin,
El Paso Community College

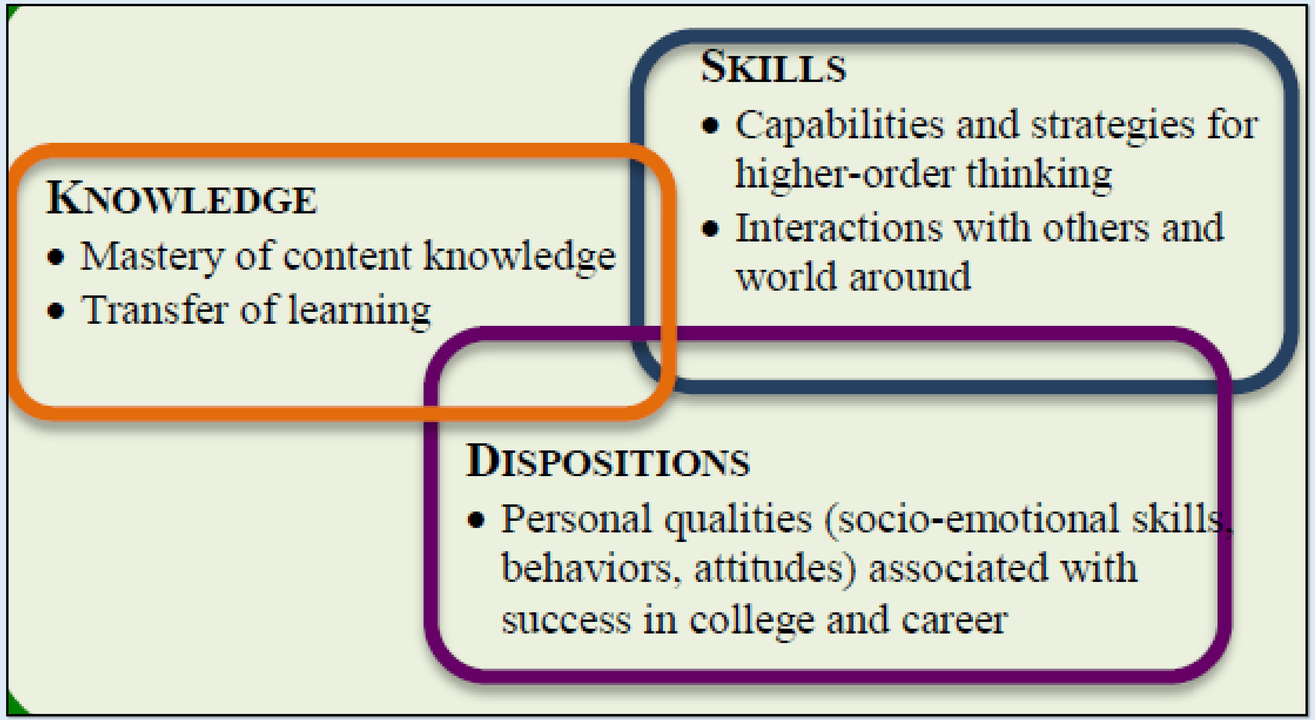
acm CCECC
Committee for Computing Education in Community Colleges

Goal

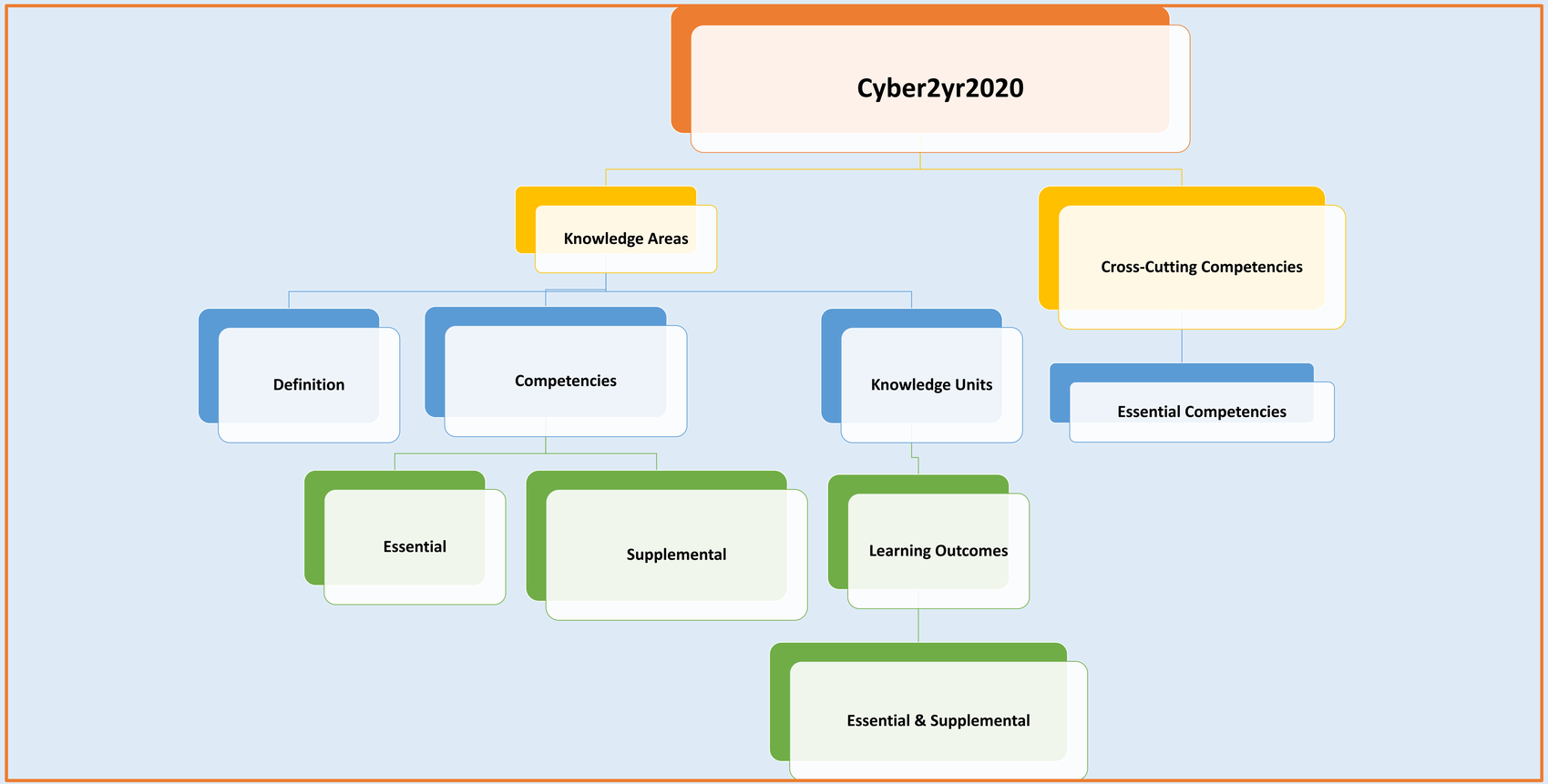
Develop curriculum guidelines for *Cybersecurity Pre-Bachelor Programs, called Cyber2yr2020* as a spin-off from CSEC2017. Map to NICE Cybersecurity Workforce Framework, ABET CAC Criteria 3 & 5 for associate programs, Center of Academic Excellence in Cyber Defense Knowledge Units and existing programs.

Focus

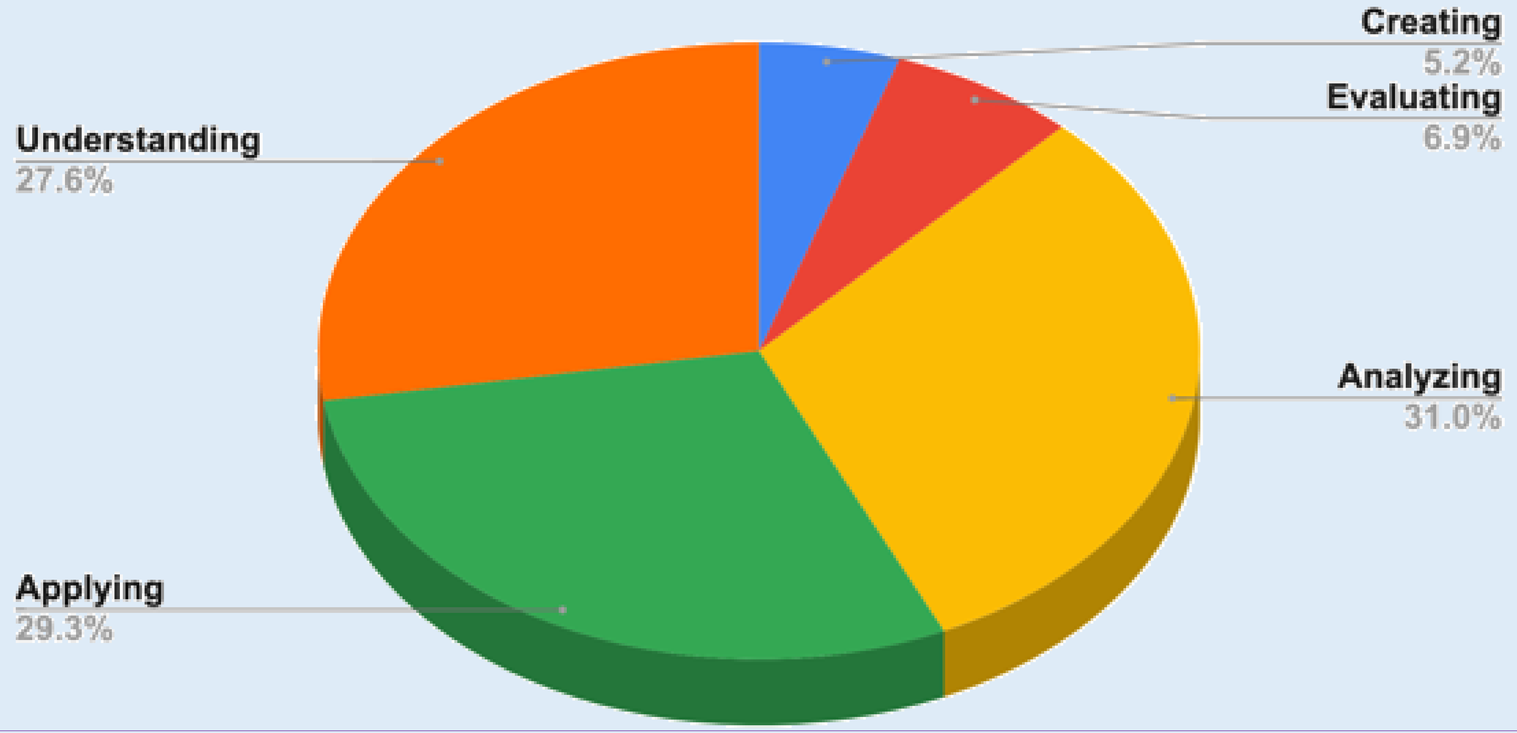
Competencies = Knowledge + Skills + Dispositions



Design


Cyber2yr2020
Knowledge Areas
Cross-Cutting Competencies
Definition
Competencies
Knowledge Units
Essential Competencies
Essential
Supplemental
Learning Outcomes
Essential & Supplemental

Bloom’s Competency Distribution



Knowledge Areas / Domains & Knowledge Units / Subdomains

Data	Cryptography Digital Forensics Data Integrity and Authentication Access Control	Secure Communication Protocols Cryptanalysis Data Privacy Information Storage Security
Software	Fundamental Principles Design Implementation Analysis and Testing	Deployment and Maintenance Documentation Ethics
Component	Component Design Component Procurement	Component Testing Component Reverse Engineering
Connection	Physical Media Hardware and Physical Component Interfaces and Connectors Distributed Systems Architecture	Network Architecture Network Implementations Network Services Network Defense
System	System Thinking System Management System Access and Control	System Testing Common System Architectures
Human	Identity Management Social Engineering Personal Compliance with Cybersecurity Rules/Policy/Ethical Norms	Awareness and Understanding Personal Data Privacy and Security Usable Security and Privacy
Organizational	Risk Management Security Governance & Policy Analytical Tools Systems Administration	Cybersecurity Planning Business Continuity, Disaster Recovery, and Incident Management Security Program Management Personnel Security
Societal	Cybercrime Cyber Law Cyber Ethics	Cyber Policy Privacy

Software Security

Definition

Focuses on the development of software with security and potential vulnerabilities in mind so that it cannot be easily exploited.

The security of a system, and of the data it stores and manages, depends in large part on the security of its software. The security of software depends on how well the requirements match the needs that the software is to address, how well the software is designed, implemented, tested, and deployed and maintained. The documentation is critical for everyone to understand these considerations, and ethical considerations arise throughout the creation, deployment, use, and retirement of software.

Essential Competencies

- [SOF-E1] Write secure code with appropriate documentation for a software system and its related data. *Applying*
- [SOF-E2] Analyze security and ethical considerations at each phase of the software development lifecycle. *Analyzing*
- [SOF-E3] Use documentation, such as third-party library documentation, in a given secure computing scenario. *Applying*

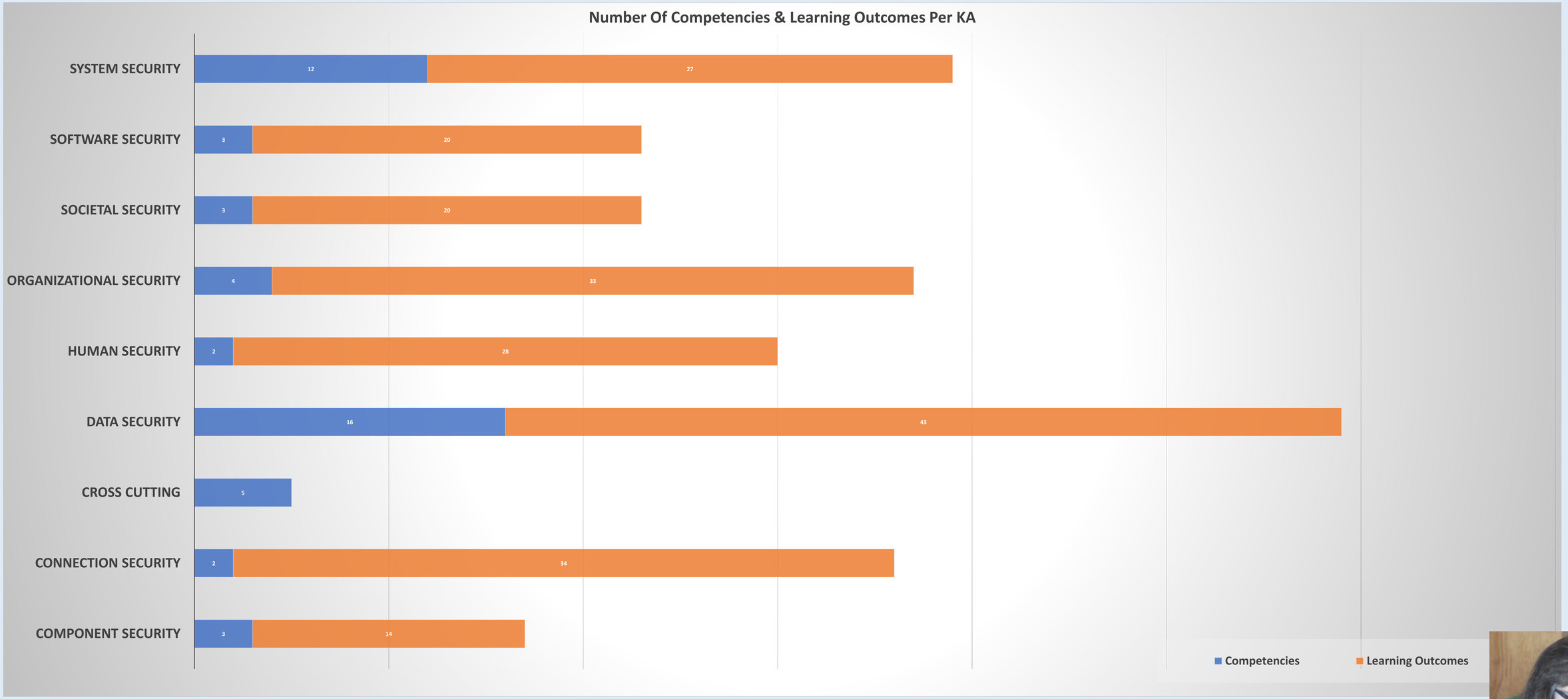
Supplemental Competencies

- [SOF-S1] Implement isolation to secure a process or application. *Applying*
- [SOF-S2] Discuss the relationship between an organization's mission and secure software design. *Understanding*
- [SOF-S3] Write software specifications, including security specifications, for a given process or application. *Applying*
- [SOF-S4] Assess a given test plan, from a security perspective. *Evaluating*
- [SOF-S5] Examine social and legal aspects of software development from a security perspective. *Analyzing*
- [SOF-S6] Develop user documentation for software installation with security appropriately included. *Creating*

Knowledge Units

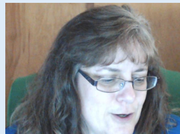
Fundamental Principles
Design
Implementation
Analysis and Testing

Deployment and Maintenance
Documentation
Ethics


Number Of Competencies & Learning Outcomes Per KA
SYSTEM SECURITY
12
27
SOFTWARE SECURITY
3
20
SOCIETAL SECURITY
3
20
ORGANIZATIONAL SECURITY
4
33
HUMAN SECURITY
2
28
DATA SECURITY
16
43
CROSS CUTTING
5
CONNECTION SECURITY
2
34
COMPONENT SECURITY
3
14
Competencies
Learning Outcomes

Rubrics

Component Security		
Emerging	**Learning Outcome - Developed**	**Highly Developed**
Component Design		
Recognize that a component's design may create vulnerabilities in information systems. *Remembering*	Discuss how a component's design may create vulnerabilities in information systems. *Understanding* [COM-LO-E01]	Illustrate how a component's design may create vulnerabilities in information systems. *Applying*
Component Procurement		
List some vulnerabilities, risks, and mitigations for components of an organizational network in a supply chain. *Remembering*	Discuss vulnerabilities, risks, and mitigations for components of an organizational network at various points in a supply chain. *Understanding* [COM-LO-E02]	Analyze vulnerabilities, risks, and mitigations for components of an organizational network at various points in a supply chain. *Analyzing*
Name some security threats and risks to hardware and software in component procurement. *Remembering*	Discuss security threats and risks to both hardware and software in component procurement, such as malware attached during manufacturing or transportation. *Understanding* [COM-LO-E03]	Outline security threats and risks to both hardware and software in component procurement. *Analyzing*
Component Testing		
Describe component security testing procedures. *Understanding*	Perform component security testing. *Applying* [COM-LO-E04]	Appraise component security testing procedures. *Evaluating*
Define unit testing and system-level testing. *Remembering*	Describe unit testing tools and techniques, as distinguished from those used in system-level testing. *Understanding* [COM-LO-E05]	Compare unit testing tools and techniques with those used in system-level testing, and the role of each in a comprehensive test plan. *Analyzing*
Component Reverse Engineering		
Recall common reverse engineering scenarios for components of a system. *Remembering*	Describe common reverse engineering scenarios for components of a system. *Understanding* [COM-LO-E06]	Perform reverse engineering on components of a system. *Applying*



Rubrics

Bluegrass Community & Technical College
Ivy Tech Community College
Lord Fairfax Community College

Highlight your Cybersecurity Program: ccecc.acm.org/correlations

Classification Mappings

- ABET 2Y Cybersecurity (CAC)
- Center of Academic Excellence in Cyber Defense (CAE-CD)
- NICE Framework Categories

More information available at

ccecc.acm.org/guidance/cybersecurity

SCAN ME