Shaping Curricular Guidelines for Associate-Degree Cybersecurity Programs

acm CCECC Committee for Computing Education in Community Colleges

Melissa Stange, Cara Tang, Christian Servin, Cindy S. Tucker, Markus Geissler

Overview of the Guidance

- **Uses the ACM *Cybersecurity Curricula 2017 (CSEC2017)* *as a starting point***
- **Includes contemporary cybersecurity concepts**
- **Identifies essential and supplemental knowledge areas for associate-level cybersecurity programs**

Driving Factors

- A top U.S. priority to build a highly capable cybersecurity workforce
- Worldwide security spending hit $96.3 billion in 2018
- 58% of business owners with up to 29 employees have been victims of cyber-attacks
- Job predictions that information security analyst will grow by 28% between 2016 and 2026
- Creation of CSEC2017

Process

Under the auspices of the ACM Education Board, the Committee for Computing Education in Community Colleges (CCECC):

Phase 1: Develop a initial draft called StrawDog February 2019

- Convened a task force of community college educator to develop the initial draft of the updated guidance
- Convened advisors from industry and universities
- Identified CSEC2017 aspects appropriateness at the junior/community college level
- Consider other influences such as CAE2Y knowledge units (KUs) - 2019 Foundational + Technical Core and professional code of ethics
- Built the guidance on a framework of learning outcomes
- Released for public review and comment

Phase 2: Develop a second draft called IronDog July 2019

- Incorporate feedback on StrawDog
- Consider additional influences such as NICE Cybersecurity Workforce Framework
- Provide competencies for each knowledge area
- Release for public review and comment

Phase 3: Final Version Q1 2020

- Incorporate feedback on IronDog
- Release for public review and comment

Knowledge Areas (KAs)

- ✓ **Data Security**
- ✓ **Software Security**
- ✓ **Component Security**
- ✓ **Connection Security**
- ✓ **System Security**
- ✓ **Human Security**
- ✓ **Organizational Security**
- ✓ **Societal Security**

Knowledge Unit (KU) Sampling

- **Cryptography**
- **Digital Forensics**
- **Data Integrity and Authentication**
- **Access Control**
- **Secure Communication Protocols**
- **Cryptanalysis**
- **Data Privacy**
- **Information Storage Security**
- **Software Analysis & Testing**
- **Ethics**
- **Component Reverse Engineering**
- **Distributed Systems Architecture**
- **Network Defense**
- **System Thinking**
- **Common System Architectures**
- **Identity Management**
- **Social Engineering**
- **Awareness and Understanding**
- **Personal Data Privacy and Security**
- **Usable Security and Privacy**
- **Risk Management**
- **Security Governance & Policy**
- **Cybersecurity Planning**
- **Cybercrime**
- **Cyber Law**
- **Cyber Policy**
- **Privacy**

Learning Outcomes Classification

- **Essential** - appropriate for all 2-year cyber programs
- **Supplemental** - appropriate for some 2-year cyber programs

Sample Learning Outcomes (LOs)

Use historical ciphers, such as shift cipher, affine cipher, substitution cipher, Vigenere cipher, ROT-13, Hill cipher, Enigma machine, and others, to encrypt and decrypt data.

Apply fundamental design principles including least privilege, open design, and abstraction

Discuss security threats and risks to both hardware and software in component procurement, such as malware attached during manufacturing or transportation.

Compare the OSI model and the TCP/IP model.

Illustrate how different management components protect the operating system from attack.

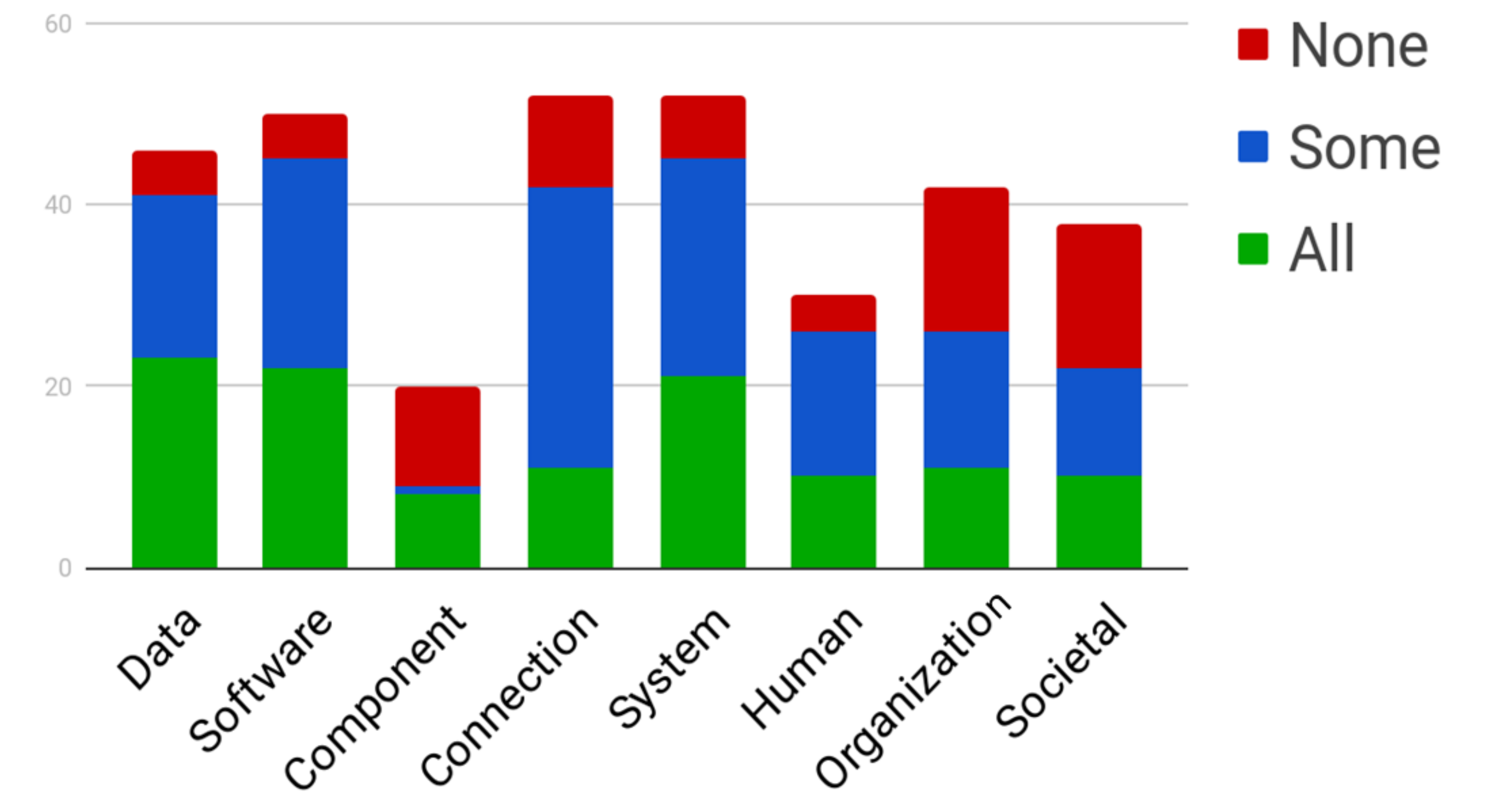
Appraise individual responsibilities related to cyber hygiene, such as password creation, maintenance, and storage; mitigation tools; identification and use of safe websites; and identifying and using appropriate privacy settings.

Summarize significant national and international laws that relate to cybersecurity.

Distinguish among ethical hacking, nuisance hacking, activist hacking, criminal hacking, and acts of war.

Investigate cultural differences in the existence of privacy norms and boundaries.

CSEC2017 Topic Inclusion



Sample Competencies

Perform major database administration tasks such as create and manage database users, roles and privileges, backup, and restore database objects to ensure organizational efficiency, continuity, and information security.

Analyze the security of a software system and its related data and apply secure programming practices.

Implement policies and procedures in accordance with national and international laws to protect information security.

Distinguish and mitigate vulnerabilities of system components.

Evaluate and describe organizational policies, rules, and norms with security implications.

Summarize the components of a business continuity plan that ensures minimal down time and quick recovery in the face of cybersecurity incidents or natural disasters.

Describe trends in human behavior which pose risks to individual and organizational privacy and security.

Contact Us

For project overview, status or to comment on IronDog, visit the project website at

ccecc.acm.org/guidance/cybersecurity