Joint Task Force (JTF) on Cybersecurity Education

http://cybered.acm.org/

Yair Levy, Diana Burley, Herb Mattord

CAE Community
Nov 8, 2018

Miami, FL

Available now!
http://cybered.acm.org

CYBERSECURITY CURRICULA 2017

Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity

A Report in the Computing Curricula Series
Joint Task Force on Cybersecurity Education

Association for Computing Machinery
IEEE computer society
ASSOCIATION FOR INFORMATION SYSTEMS
ifip

Sponsors

- Association for Computing Machinery (ACM)
- IEEE Computer Society (IEEE-CS)
- Association for Information Systems Special Interest Group on Security and Privacy (AIS SIGSEC)
- International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8)

- US National Science Foundation (Award 1623104)
- Intel
- US National Security Agency (Grant H98230-17-1-0219)

JTF Members

Diana Burley, Co-Chair, The George Washington University

Matt Bishop, Co-Chair, University of California Davis

Scott Buck, Intel Labs

J Ekstrom, Brigham Young University

Lynn Fletcher, Nelson Mandela Metropolitan University, South Africa

David Gibson, U.S. Air Force Academy

Beth Hawthorne, Union County College

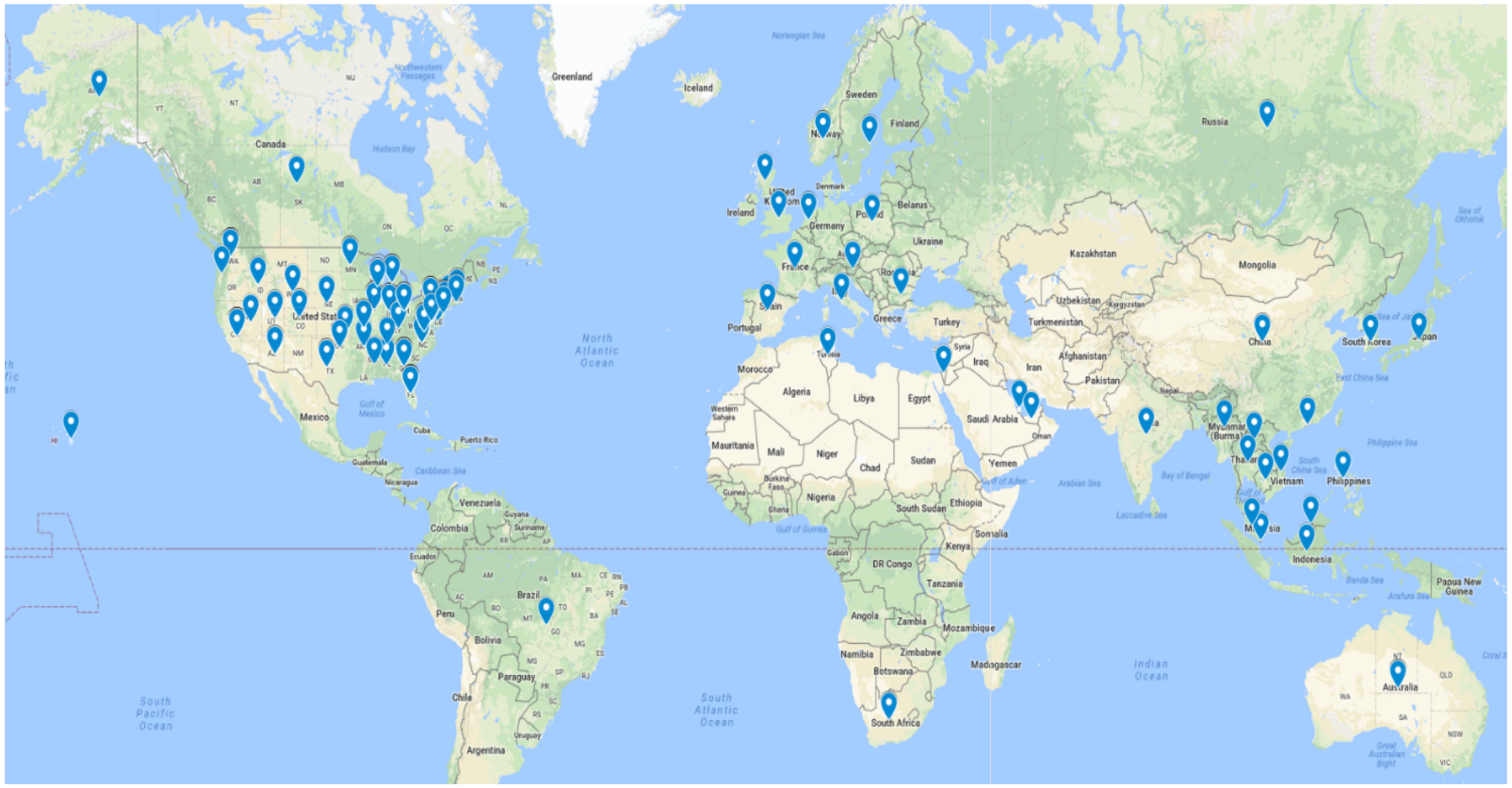
Sidd Kaza, Towson University

Yair Levy, Nova Southeastern University

Herb Mattord, Kennesaw State University

Allen Parish, U.S. Naval Academy

Developed with the assistance of > 325 contributors across 35 countries, CSEC2017 is the first set of global cybersecurity curricular guidelines and we envision that it will be the leading resource of comprehensive curricular content for global institutions seeking to develop a broad range of cybersecurity offerings.



CSEC2017 Mission

- To develop comprehensive and flexible undergraduate curricular guidance in cybersecurity education that will support future program development and associated educational efforts at the post-secondary level.

- To produce a curricular volume that structures the cybersecurity discipline and provides guidance to institutions seeking to develop or modify a broad range of programs rather than a prescriptive document to support a single program type.

CSEC2017 Goals

- To describe a vision of proficiency in cybersecurity;
- To define a structure for the cybersecurity discipline by developing a thought model that defines the boundaries of the discipline and outlines key dimensions of the curricular structure;
- To support the alignment of academic programs and industry needs in cybersecurity;
- To involve broad global audience of stakeholders through continuous community engagement during the development process;
- To develop curricular guidance that is comprehensive enough to support a wide range of program types; and
- To develop curricular guidance that is grounded in fundamental principles that provide stability, yet is structured to provide flexibility to support evolving program needs.

CSEC2017 Purpose

WHAT

- To develop course roadmaps that link the forthcoming CSEC2017 Curricular Guidance to the National Cybersecurity Workforce Framework (NCWF).

WHY

- To aid program developers bridge the academic program to workforce gap

HOW

- By linking CSEC2017 learning outcomes with NCWF specialty area competencies through roadmap exemplars that identify and describe relevant courses and course modules; outline knowledge acquisition strategies when specific courses are not available within the institution; and highlight challenges (and associated strategies to overcome them) to linking the CSEC2017 and the NCWF for the specialty area.

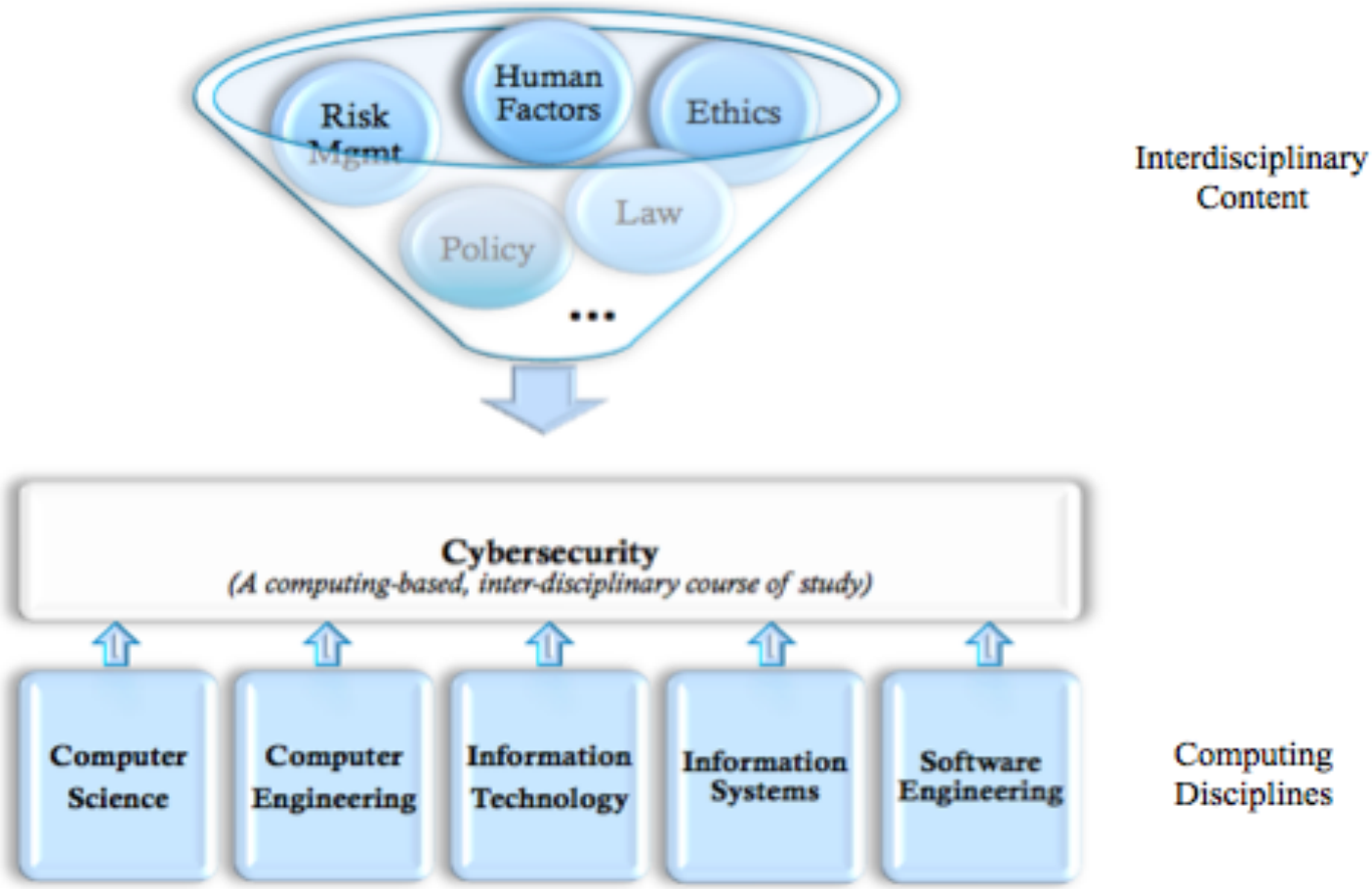
CSEC2017 Guiding Principles

Cybersecurity education programs should:

- Be based on core knowledge and skills
- Have a computing-based foundation
- Teach concepts applicable to a broad range of cybersecurity expertise
- Emphasize ethical obligations and responsibilities
- Be flexible so programs can tailor their curriculum to any specialized needs

Cybersecurity is defined as

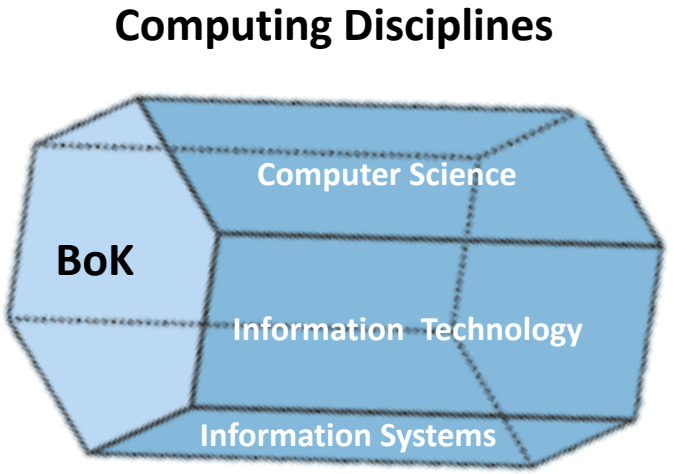
a computing-based discipline involving technology, people, information, and processes to enable assured operations in the ***context of adversaries****. It involves the creation, operation, analysis, and testing of secure computer systems. It is an* ***interdisciplinary*** *course of study, including aspects of law, policy, human factors, ethics, and risk management*.


Risk Mgmt
Human Factors
Ethics
Law
Policy
...
Cybersecurity
(A computing-based, inter-disciplinary course of study)
Computer Science
Computer Engineering
Information Technology
Information Systems
Software Engineering
Interdisciplinary Content
Computing Disciplines

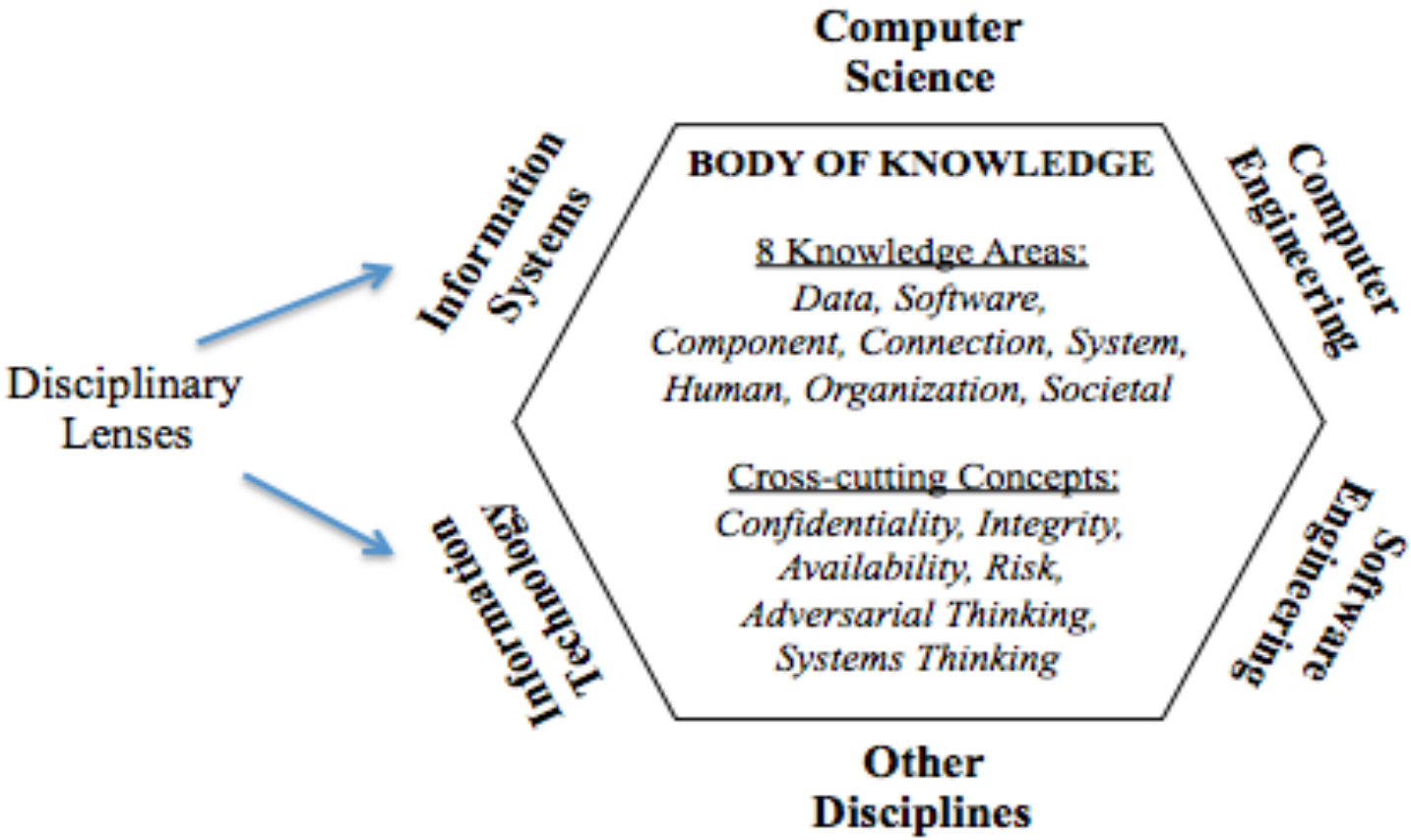
Disciplinary Lens

- The depth of coverage across KUs, topics, and learning outcomes will be determined by the combination of Disciplinary Lens and Institution Type

- ACM/IEEE Disciplines
  - Computer Science
  - Information Technology
  - Computer Engineering
  - Software Engineering
  - Information Systems
  - (Plus) Other Disciplines



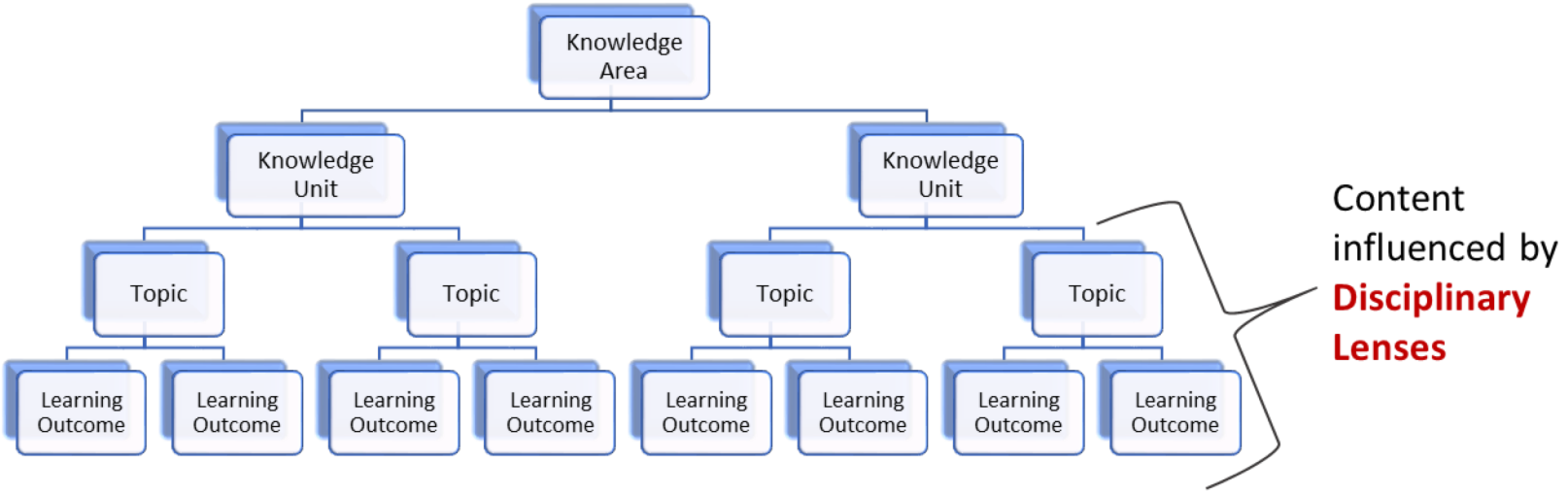
CSEC2017 Thought Model



CSEC2017 Knowledge Areas

1. Data Security
2. Software Security
3. Component
4. Connection Security
5. System Security
6. Human Security
7. Organizational Security
8. Societal Security

Knowledge Area Organization



Knowledge Area Descriptions

- **Data Security:** focuses on the protection of data at rest, during processing, and in transit.

- **Software Security:** focuses on the development and use of software that reliably preserves the security properties of the information and systems it protects.

- **Component Security:** focuses on the design, procurement, testing, analysis and maintenance of components integrated into larger systems.

- **Connection Security:** focuses on the security of the connections between components including both physical and logical connections.

Knowledge Area Descriptions (continued)

- **System Security:** focuses on the security aspects of systems that are composed of components and connections, and use software.

- **Human Security:** focuses on protecting individuals' data and privacy in the context of organizations (i.e., as employees) and personal life, in addition to the study of human behavior as it relates to cybersecurity.

- **Organizational Security:** focuses on protecting organizations from cybersecurity threats and managing risk to support the successful accomplishment of the organization's mission.

- **Societal Security:** focuses on aspects of cybersecurity that broadly impact society as a whole for better or for worse.

Knowledge Area Essentials

- The essential concepts of each knowledge area capture the cybersecurity proficiency that every student needs to achieve regardless of program focus.
- Essentials should be introduced early and reinforced throughout every cybersecurity program.
- These concepts may also appear as specific knowledge units, as topics within knowledge units, or as aggregates of topics across knowledge units. Taken together, the essential concepts in all of the knowledge areas should be covered in every cybersecurity program.
- In the curricular volume, the essential concepts are explicitly identified for each knowledge area along with learning outcomes.

Essentials

Data Security Essentials

- Basic cryptography concepts
- End-to-end secure communications
- Digital forensics
- Data integrity and authentication
- Data erasure

Software Security Essentials

- Fundamental design principles; least privilege, open design, and abstraction
- Security requirements and the roles they play in design
- Implementation issues
- Static, dynamic analysis
- Configuring, patching
- Ethics, especially in development, testing, and vulnerability disclosure

Essentials (continued)

Component Security Essentials

- Vulnerabilities of system components
- Component lifecycle
- Secure component design principles
- Supply chain management
- Security testing
- Reverse engineering

Connection Security Essentials

- Systems, architecture, models, and standards
- Physical component interfaces
- Software component interfaces
- Connection attacks
- Transmission attacks

Essentials (continued)

System Security Essentials

- Holistic approach
- Security policy
- Authentication
- Access control
- Monitoring
- Recovery
- Testing
- Documentation

Human Security Essentials

- Identity management
- Social engineering
- Awareness and understanding
- Social behavioral privacy and security
- Personal data privacy and security

Essentials (continued)

Organizational Security Essentials

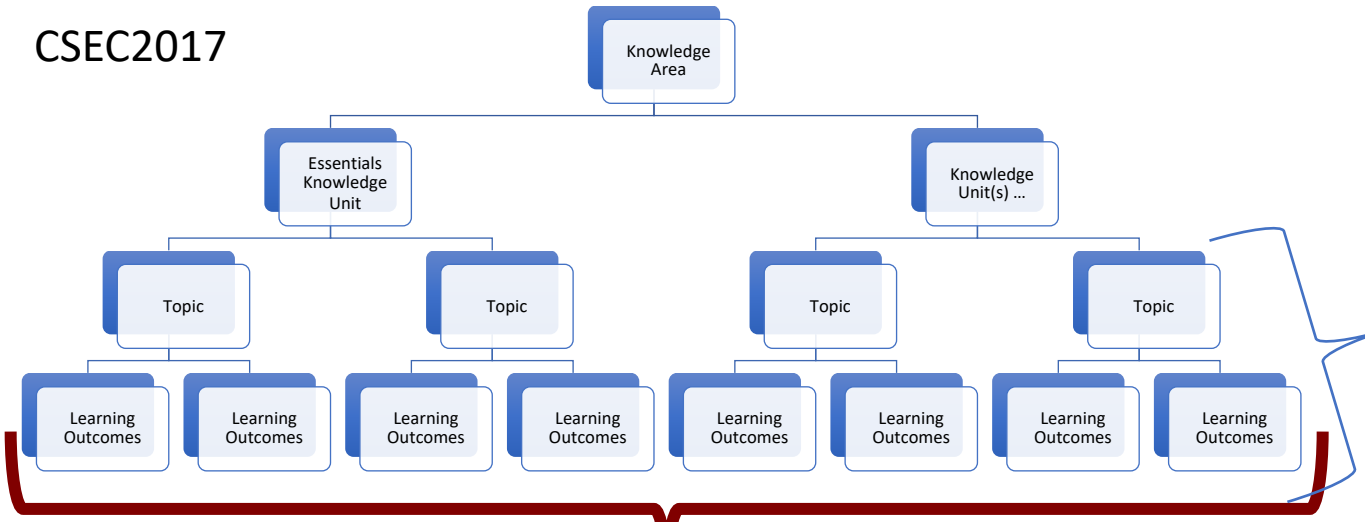
- Risk management
- Governance and policy
- Laws, ethics, and compliance
- Strategy and planning

Societal Security Essentials

- Cybercrime
- Cyber law
- Cyber ethics
- Cyber policy
- Privacy

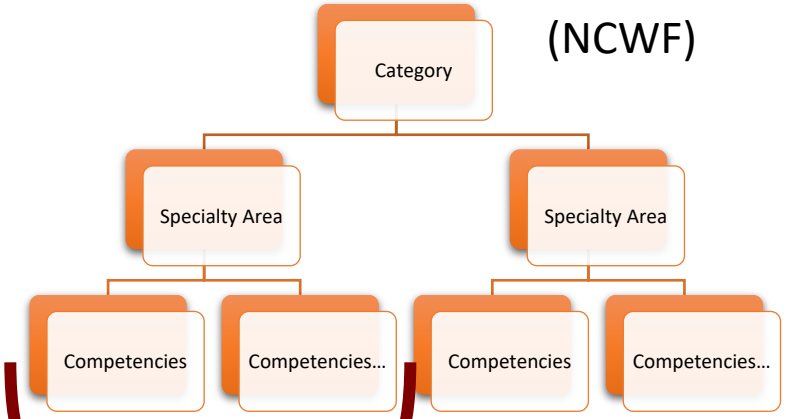
Linking Learning Outcomes & Competencies

CSEC2017



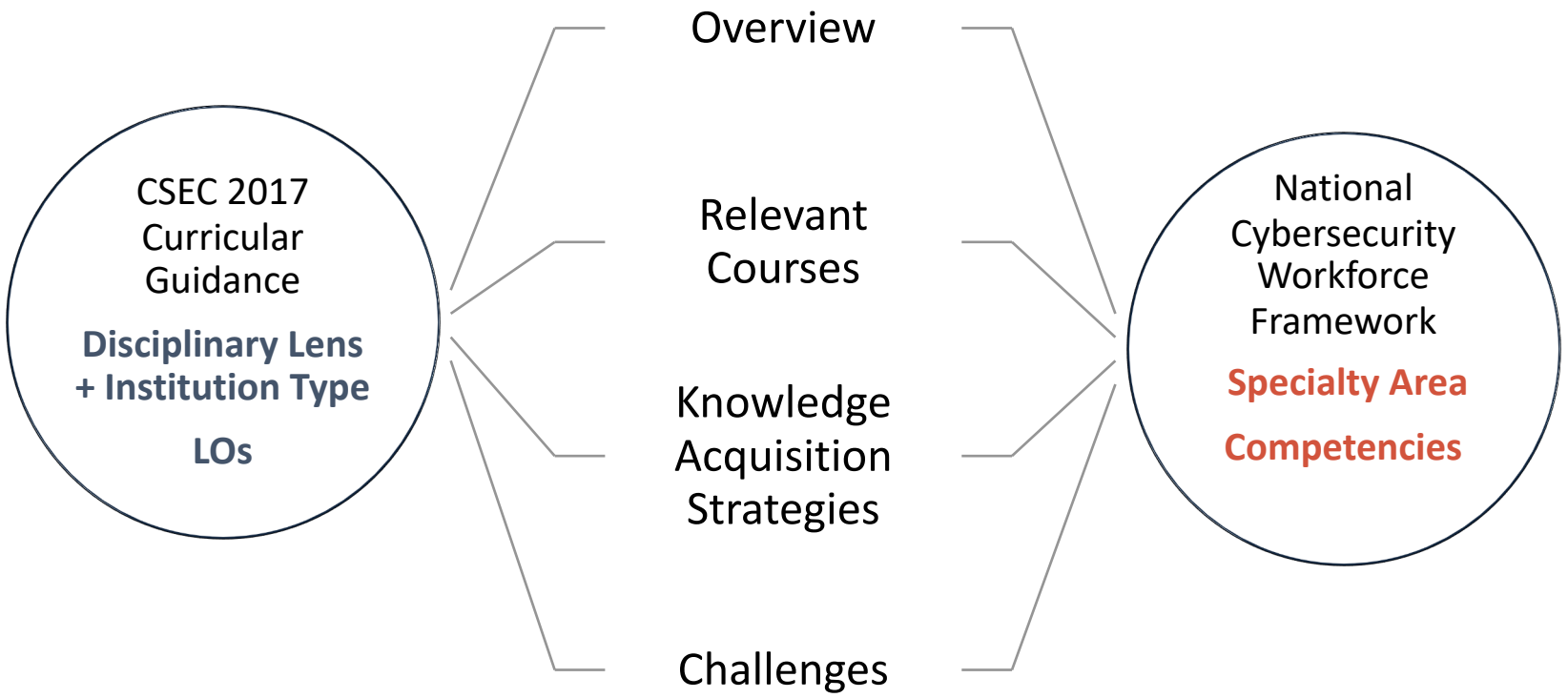
Content influenced by disciplinary lens and institution type

National Cybersecurity Workforce Framework (NCWF)



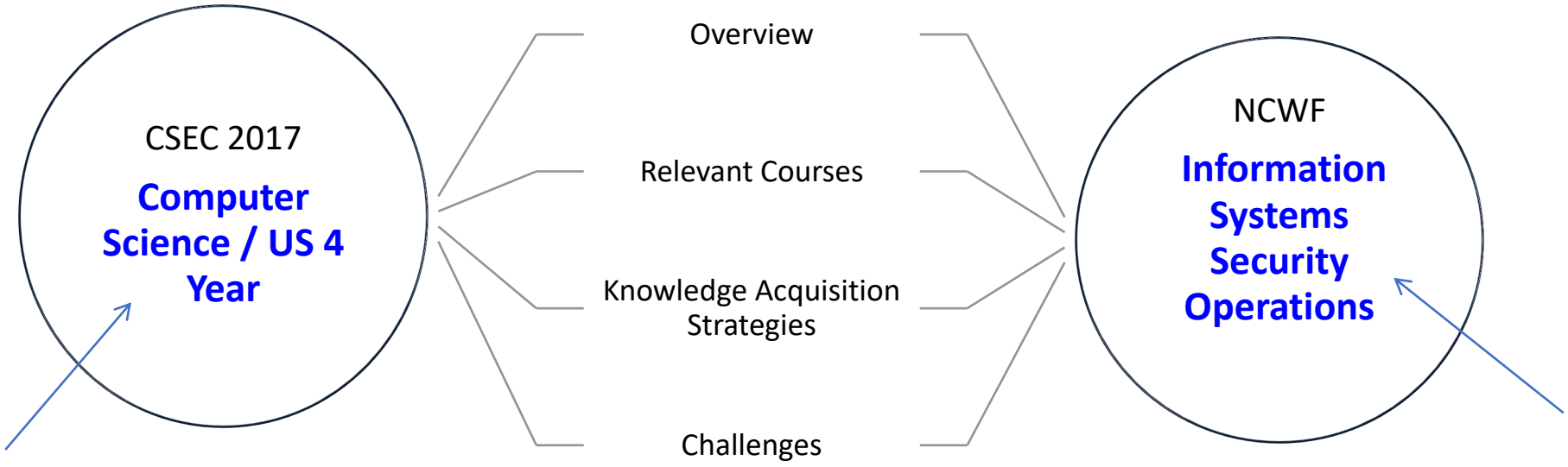
Roadmaps link LOs to Specialty Area Competencies

Roadmap Components



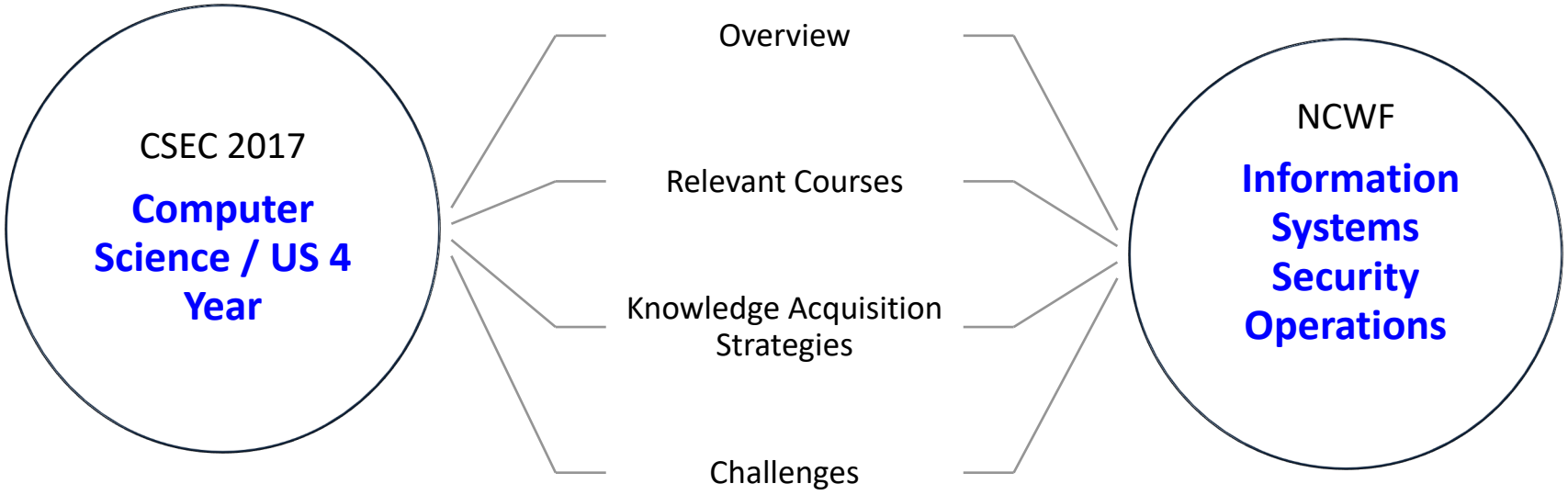
Roadmap Development Process

STEP 1: Identify type of program (Disciplinary Lens + Institution Type) and desired student outcome (NCWF Specialty Area)



Roadmap Development Process

STEP 2: Link 8 KA Essential Knowledge Unit LOs to NCWF Specialty Area Competencies

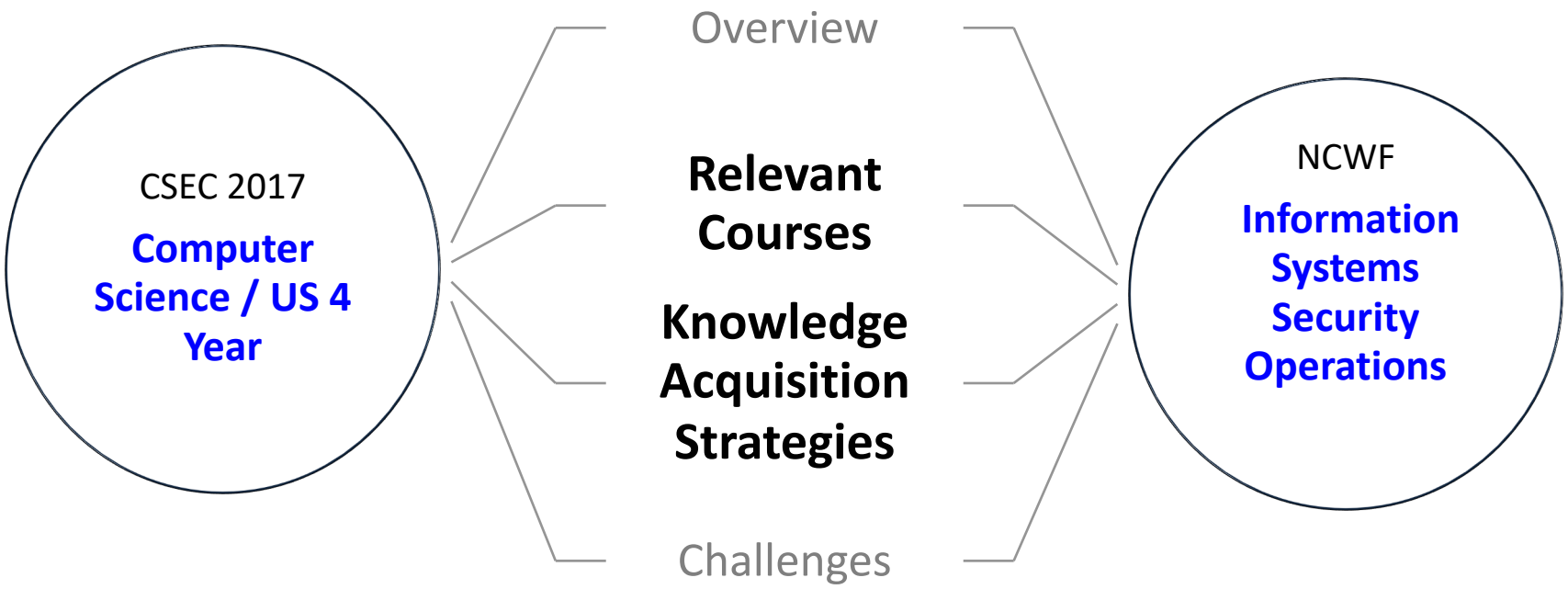


CS/US 4 Year
8 KA Essential
Knowledge Unit LOs

ISSO
Competencies

Roadmap Development Process

STEP 3: identify knowledge acquisition strategies (courses, informal learning opportunities at the institution)



Roadmap Development Process

STEP 4: Outline institutional challenges (e.g. gaps in courses) to meeting competency requirements

Exemplars

- The CSEC2017 Body of Knowledge affords the flexibility to support many different types of programs. The exemplars will demonstrate how a variety of institutions cover the knowledge area essentials and some subset of the knowledge units.
- Appendix C of the curricular volume contains the Curricular, Workforce, and Course exemplar templates
- The exemplars will be provided on the cybered.acm.org community engagement website to demonstrate the ways that the Body of Knowledge may be organized into a complete curriculum.

Curricular Exemplar Requirements

- Institution information
- Disciplinary Lens of program
- Curricular overview
- Possible curricular revisions (based on CSEC2017)
- Course summaries
- Knowledge Unit Table with course outcomes (spreadsheet)
- Essentials and Knowledge Unit Coverage Table (spreadsheet)

Disciplinary Lens + Institution Type

Program exemplars in each category will provide details on depth of coverage and learning outcomes.

		Institution Type		
		US 4 Year	US 2 Year	Non-US
Disciplinary Lens	Computer Science			
	Computer Engineering			
	Software Engineering			
	Information Systems			
	Information Technology			
	Other Disciplines			

Contact the JTF if you are interested in developing an exemplar.

Example: Knowledge Unit Table w/Outcomes

Knowledge Areas	Knowledge Units	COSC310 - Special Topics Advanced Programming	COSC418 - Ethical and Societal Concerns of Computer Scientists	COSC440 - Operating System Security	COSC450 - Network Security	COSC458 - Application Software Security	COSC481 - Case Studies in Computer Security	COSC485 - Reverse Engineering and Malware Analysis	MATH/COSC314 - Cryptography
Data Security	Essentials			Describe the purpose of cryptography and list ways it is used in data communications; Explain how public key infrastructure supports digital signing and encryption and discuss the limitations/vulnerabilities. Describe which cryptographic protocols, tools and techniques are appropriate for a given situation;	Describe the purpose of cryptography and list ways it is used in data communications; Explain how public key infrastructure supports digital signing and encryption and discuss the limitations/vulnerabilities. Describe which cryptographic protocols, tools and techniques are appropriate for a given situation; Explain the goals of end-to-end data security;	Describe the purpose of cryptography and list ways it is used in data communications; Explain how public key infrastructure supports digital signing and encryption and discuss the limitations/vulnerabilities. Describe which cryptographic protocols, tools and techniques are appropriate for a given situation;	Explain how public key infrastructure supports digital signing and encryption and discuss the limitations/vulnerabilities. Describe which cryptographic protocols, tools and techniques are appropriate for a given situation;	Explain how public key infrastructure supports digital signing and encryption and discuss the limitations/vulnerabilities. Describe which cryptographic protocols, tools and techniques are appropriate for a given situation;	Describe the purpose of cryptography and list ways it is used in data communications; Describe the following terms: cipher, cryptanalysis, cryptographic algorithm, and cryptology, and describe the two basic methods (ciphers) for transforming plaintext in ciphertext; Explain how public key infrastructure supports digital signing and encryption and discuss the limitations/vulnerabilities. Understand the dangers of inventing one's own cryptographic methods. Describe which cryptographic protocols, tools and techniques are appropriate for a given situation; Explain the goals of end-to-end data security;

Example: Essentials and KU Coverage Table

Knowledge Areas	Knowledge Units	COSC310 - Special Topics Advanced Programming	COSC418 - Ethical and Societal Concerns of Computer Scientists	COSC440 - Operating System Security	COSC450 - Network Security	COSC458 - Application Software Security	COSC481 - Case Studies in Computer Security	COSC485 - Reverse Engineering and Malware Analysis	MATH/COSC314 - Cryptography	% of Coverage	Optional: Additional Topics
Data Security	Essentials			Basic cryptography concepts; Data integrity and authentication; Information storage security;	Basic cryptography concepts; Digital forensics; End to end secure communication; Data integrity and authentication; Information storage security	Basic cryptography concepts; Data integrity and authentication; Information storage security;	Data integrity and authentication; Information storage security;	Digital forensics; Data integrity and authentication; Information storage security;	Basic cryptography concepts; End-to-End secure communication; Data integrity and authentication;	*100%*	
	Cryptography			Basic concepts	Basic concepts; Mathematical background; Symetric ciphers; Asymetric ciphers;				Basic concepts; Advanced concepts; Mathematical background; Historical ciphers; Symetric (private key) ciphers; Asymetric (public-key) ciphers;	100%	

Continued Community Engagement

- Community website: cybered.acm.org
  - Downloadable CSEC2017 document
  - Information about the Task Force and its process
  - Curriculum, Course, and Workforce exemplars (solicitation)
  - Exemplar templates and submission information
  - List of past and upcoming community engagement events

Joint Task Force (JTF) on Cybersecurity Education

http://cybered.acm.org/

Thank YOU!

Questions?

Comments?

Feedback?