Public Review and Comment period: January 14 – February 14, 2017
Provide feedback at: http://csec2017.org

Cybersecurity Curricula 2017

Curriculum Guidelines for Undergraduate Degree Programs in Cybersecurity

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

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

Version 0.5 Report
14 January 2017

ISBN: <to be determined>
DOI: <to be determined>
Web link: <http:// to be determined>
ACM Order Number: <to be determined>

When available, you may order additional copies from:

ACM Order Department
P.O. Box 30777
New York, NY 10087-0777
IEEE Computer Society
Customer Service Center
10662 Los Vaqueros
P.O. Box 3014
Los Alamitos, CA 90720-1314
+1-800-342-6626
+1-212-626-0500 (outside U.S.)
orders@acm.org
Tel: +1 800 272 6657
Fax: +1 714 821 4641
http://computer.org/cspress
csbook@computer.org

Sponsors:

This report was made possible by financial support from the following:
Association for Computing Machinery (ACM)
IEEE Computer Society (IEEE-CS)
Association for Information Systems Special Interest Group on Security (AIS SIGSEC)

The US National Science Foundation
Intel Corporation

The CSEC2017 Final Report has been endorsed by <to be determined>.

Cybersecurity Curricula 2017

Version 0.5 Report
14 January 2017

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

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

CSEC2017 Joint Task Force

Diana L. Burley, Ph.D. (JTF Co-Chair, ACM/CEP)
Professor, Human & Organizational Learning
Executive Director, Institute for Information Infrastructure Protection
The George Washington University, USA

Matt Bishop, Ph.D. (JTF Co-Chair, ACM/IFIP)
Professor, Computer Science
Co-Director, Computer Security Laboratory
University of California, Davis, USA

Scott Buck (ACM/CEP)
University Program Director
Intel Corporation, USA

Joseph J. Ekstrom, Ph.D. (IEEE CS)
Associate Professor, Information Technology
Brigham Young University, USA

Lynn Futcher, Ph.D. (ACM/IFIP)
Associate Professor
Nelson Mandela Metropolitan University, South Africa

Col. David Gibson, Ph.D. (ACM/CEP)
Professor, Computer Science
Chair, Department of Computer Science
United States Air Force Academy, USA

Elizabeth Hawthorne, Ph.D. (ACM/CEP)
Senior Professor, Computer Science
Union County College, USA

Siddharth Kaza, Ph.D. (ACM)
Associate Professor, Computer & Information Science
Chair, Department of Computer & Information Science
Towson University, USA

Yair Levy, Ph.D. (AIS SIGSEC)
Professor, Information Systems and Cybersecurity
Director, Center for e-Learning Security Research (CeLSR)
Nova Southeastern University, USA

Herbert Mattord, Ph.D. (AIS SIGSEC)
Associate Professor, Information Systems
Associate Director, Center for Information Security Education
Kennesaw State University, USA

Allen Parrish, Ph.D. (IEEE CS/CEP)
Professor, Cyber Science
Chair, Department of Cyber Science
United States Naval Academy, USA

Table of Contents

Chapter 1: Introduction

For nearly five decades, starting with Computer Science 1968[1], the ACM education initiative has collaborated with other professional and scientific societies to establish curricular guidelines for academic program development in the computing disciplines. Currently, ACM curricular volumes provide recommendations in computer science, computer engineering, information systems, information technology, and software engineering. The ACM Computing Curricula 2005 (CC2005) report provides an overview of the curriculum guidelines for each of these five computing disciplines[2]. This volume, CSEC2017, represents an expansion of the ACM education initiative to include the first set of global curricular recommendations in cybersecurity education.

By all accounts, the world faces a current and growing workforce shortage of qualified cybersecurity professionals and practitioners. In fact, both government and non-government sources project nearly 1.5 million cybersecurity-related positions going unfilled by 2020[3]. The workforce demand is acute, immediate, and growing[4]. In order to develop the required talent, academic departments across the spectrum of computing disciplines are launching initiatives to establish cybersecurity programs. These institutions need curricular guidance based on a comprehensive view of the cybersecurity field, the specific demands of the base discipline, and the relationship between the curriculum and cybersecurity workforce frameworks.

In August 2015, the ACM Education Board recognized this urgent need and took measures to assemble a Joint Task Force on Cybersecurity Education (CSEC2017) with other professional and scientific computing societies to develop comprehensive curricular guidance in cybersecurity education.

1.1 Background

The CSEC2017 Joint Task Force on Cybersecurity Education (JTF) was officially launched in September 2015 as a collaboration between major international computing societies: Association for Computing Machinery (ACM), IEEE Computer Society (IEEE CS)[5], Association for Information Systems Special Interest Group on Security (AIS SIGSEC)[6], and International Federation for Information Processing Technical Committee on Information Security Education (IFIP WG 11.8)[7].

[1] ACM Curriculum Committee on Computer Science. 1968. Curriculum 68: Recommendations for Academic Programs in Computer Science. *Comm. ACM* 11, 3 (Mar. 1968), 151-197. http://acm.org/education/curricula-recommendations

[2] Academic Programs in Computer Science. http://acm.org/education/curricula-recommendations

[3] See, for example, CSO Online: http://www.csoonline.com/article/2953258/it-careers/cybersecurity-job-market-figures-2015-to-2019-indicate-severe-workforce-shortage.html

[4] (ISC)2 Report available here: https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-(ISC)%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf

[5] IEEE CS website: https://www.computer.org/

[6] AIS SIGSEC website: http://aisnet.org/group/SIGSEC

[7] IFIP WG 11.8 website: https://www.ifiptc11.org/wg118

The ACM Education Board appointed the CSEC2017 JTF co-chairs. In addition to the co-chairs, the CSEC2017 JTF includes nine leading cybersecurity professionals selected by the participating professional societies to represent their constituencies and to provide a diverse set of perspectives. The JTF members are listed along with their affiliations at the beginning of this document.

The CSEC2017 JTF is an outcome of the Cyber Education Project (CEP)[8]. The CEP initiative was organized in July 2014 by a group of computing professionals who represented a diverse cross-section of academic institutions and professional societies. The CEP mission was two-fold: to initiate the processes for (1) developing undergraduate curricular guidance; and (2) establishing a case for the accreditation of educational programs in the "Cyber Sciences."

The term "Cyber Sciences" reflects a collection of computing-based disciplines involving technology, people, and processes aligned in a way to enable "assured operations" in the presence of risks and adversaries. It involves the creation, operation, analysis, and testing of secure computer systems (including network and communication systems) as well as the study of how to employ operations, reasonable risk taking, and risk mitigations. The concept of "Cyber Sciences" refers to a broad collection of such programs, and disciplines under this umbrella often also include aspects of law, policy, human factors, ethics, risk management, and other topics directly related to the success of the activities and operations dependent on such systems, many times in the context of an adversary.

The CSEC2017 JTF is advancing the first mission of the CEP – to develop comprehensive curricular guidance in cybersecurity education that will support future program development and associated educational efforts at the post-secondary level. While the CSEC2017 JTF has chosen to use the more generally accepted term "cybersecurity" instead of "cyber sciences" to label this effort, conceptually the terms are consistent. The precise definition of cybersecurity used to drive the CSEC2017 effort is provided below.

1.2 Vision, Mission, and Goals

The CSEC2017 JTF has worked actively since its inception in September of 2015 to define project parameters and establish a foundational vision, mission and goals. The project vision is:

> *The CSEC2017 curricular volume will be the leading resource of comprehensive cybersecurity curricular content for global academic institutions seeking to develop a broad range of cybersecurity programs at the post-secondary level.*

The CSEC2017 mission is twofold:

[8] Cyber Education Project website: http://cybereducationproject.org/about/

- 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.

Based on this mission, the CSEC2017 JTF established the following goals for the curricular volume:

- 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.

In order to further focus the content and structure included in the cybersecurity curricular guidance, the CSEC2017 JTF defined a primary and secondary audience. The primary audience is those individuals who will use the volume to establish post-secondary cybersecurity programs in computing disciplines. The secondary audience includes all other stakeholders as outlined below.

Primary audience:

- Faculty members in computing-based disciplines at academic institutions around the world who are developing or will develop cybersecurity degree programs.

Secondary audience:

- Industry members who will assist with cybersecurity program development within academic institutions, develop industry-based programs, and be consumers of the student outcomes of these programs;
- Training and professional development providers;

- Faculty members in non-computing based disciplines who are developing/or intend to develop allied programs that teach cybersecurity concepts and skills;
- Workforce framework developers (government and non-government);
- Policymakers;
- Members of the K-12 educational community who are preparing students to enter post-secondary education in cybersecurity; and
- Other stakeholders involved with cybersecurity workforce development initiatives.

1.2 Overall Scope of Cybersecurity

The CSEC2017 JTF defines cybersecurity 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.*

In the CC2005 Overview Report, the ACM identifies five primary computing disciplines, and recognizes a category of computing disciplines that highlights the increasing number of hybrid or interdisciplinary courses of study.

- Computer Engineering
- Computer Science
- Information Systems
- Information Technology
- Software Engineering
- Mixed Disciplinary Majors *(xx Informatics or Computational xx)*

The CSEC2017 JTF positions cybersecurity as a second-order computing discipline in which the approach to the curricular content is directly shaped by the computing discipline that serves as the foundation of the cybersecurity degree program. In other words, although the topics covered within the curriculum are the same, the depth of coverage and the desired student learning outcomes may differ based on the disciplinary foundation (e.g. computer science vs. information systems). The manner in which the disciplinary lens shapes the curricular content will be fully described in chapters 3 and 4 of this document.

1.3 Guiding Principles and Community Engagement

The CSEC2017 JTF has continuously engaged the broad stakeholder community throughout the development process. Community members have provided input to shape the approach, content and organizational structure of the CSEC2017 report. Community engagement activities have included: special sessions, panels and workshops at conferences affiliated with participating professional societies, international conferences, keynote addresses, webinars, working group meetings, government briefings, and information gathering sessions with an industry advisory board.

Among these activities, two key milestones in the development process were the International Security Education Workshop and the Global Stakeholder Survey. They are summarized below. A full list of community engagement activities, along with updates on the development process, and information about opportunities for continued engagement are available through the CSEC2017 website[9].

1.3.1 International Security Education Workshop

The 2016 International Security Education Workshop (ISEW) was held June 13-15th, 2016 in Philadelphia, PA[10]. The workshop was structured to advance the CSEC2017 development process. Through panel discussions and working group sessions, approximately 75 stakeholders from the global cybersecurity education community provided input on the curricular content and structure by debating two key questions:

- What should be included in a cybersecurity degree program?
- How should the volume of curricular recommendations be organized and disseminated?

The full meeting report is available on the CSEC2017 website. The input gathered from participants of the ISEW informed the first version of the CSEC2017 thought model and served as the basis of the global stakeholder survey.

1.3.2 Global Stakeholder Survey

In September 2016, after a year of community engagement and developmental work, the JTF launched a global stakeholder survey to solicit feedback on the proposed curricular thought model. Stakeholders were invited to participate in the survey through direct invitations, announcements in public educational and scientific forums, social media

[9] CSEC2017 website: http://csec2017.org
[10] The ISEW was co-located with the Colloquium for Information Systems Security Education (CISSE), and sponsored by the Intel Corporation, the National Science Foundation (NSF), and the Institute for Information and Infrastructure Protection (I3P) at the George Washington University (GW).

outreach via the JTF website and LinkedIn, and invitations sent through the distribution lists of participating professional associations. The survey yielded 231 responses from stakeholders located in 20 countries; working across academia, industry and government; and representing all five computing disciplines.

In summary, survey respondents suggested that the JTF clarify the intended audience of the curricular volume; refine the definitions and distinguish between the curricular elements of the thought model; provide additional information on the content of each of the knowledge categories; simplify the thought model; and adapt the structure to allow for placement of emerging topics. The JTF used these comments to revise the thought model. The full survey report is available on the CSEC2017 website.

1.3.3 Contributor Acknowledgement

The JTF gratefully acknowledges the valuable contributions of participants in our community engagement efforts. The list of contributors appears in an appendix at the end of this document. Opportunities to support the work of the CSEC2017 JTF are ongoing.

1.4 Structure of the Cybersecurity 2017 Report

This report, CSEC2017, presents the work of the JTF. The CSEC2017 report provides an overview of the cybersecurity discipline to frame the curricular model. The document then presents the curricular framework and outlines the recommended curricular content. Next, and in order to place the content within the larger context, the report highlights industry perspectives on cybersecurity. Finally, to aid with implementation, the report discusses issues related to the educational practice, suggests roadmaps for implementing the cybersecurity curricular framework, and includes exemplars to assist with institutional implementation.

CSEC2017 v. 0.5 is presented to the stakeholder community for review and comment. As a draft, not all sections of the report are fully developed. However, the JTF appreciates feedback on all portions of the report. Please submit all feedback using the comment form located at csec2017.org.

Chapter 2: The Cybersecurity Discipline

Cybersecurity is a computing-based discipline involving technology, people, information, and processes to enable assured operations in the context of adversaries. It draws from the foundational fields of information security and information assurance; and began with more narrowly focused field of computer security. The need for cybersecurity arose when the first mainframe computers were developed. Multiple levels of security were implemented to protect these devices and the missions they served. The growing need to maintain national security eventually led to more complex and technologically sophisticated security safeguards. During the early years, cybersecurity as practiced, even if not specifically identified as such, was a straightforward process composed predominantly of physical security and document classification. The primary threats to security were physical theft of equipment, espionage against products of the systems, and sabotage.

During the Cold War beginning in the late 1940s, many more mainframe computers were brought online to accomplish more complex and sophisticated tasks. Department of Defense's Advanced Research Projects Agency (ARPA) began examining the feasibility of a redundant, networked communications system to support the exchange of computer data. ARPANET saw wider use, increasing the potential for its misuse. Security that went beyond protecting the physical location of computing devices effectively began with a single paper published by the RAND Corporation in February 1970 for the Department of Defense. That report, RAND Report R-609, attempted to define the multiple controls and mechanisms necessary for the protection of a computerized data processing system.

In the early 1980s, the development of TCP (the Transmission Control Protocol) and IP (the Internet Protocol) led to the emergence of the Internet brought the networking aspects of Cybersecurity to the fore. The U.S. Government passed several key pieces of legislation that formalized the recognition of computer security as a critical issue for federal information systems including the Computer Fraud and Abuse Act of 1986 and the Computer Security Act of 1987. The Internet eventually brought pervasive connectivity to virtually all computers where integrity and confidentiality were a lower priority than the drive for availability where many problems that plague the Internet today result from this early lack of security.

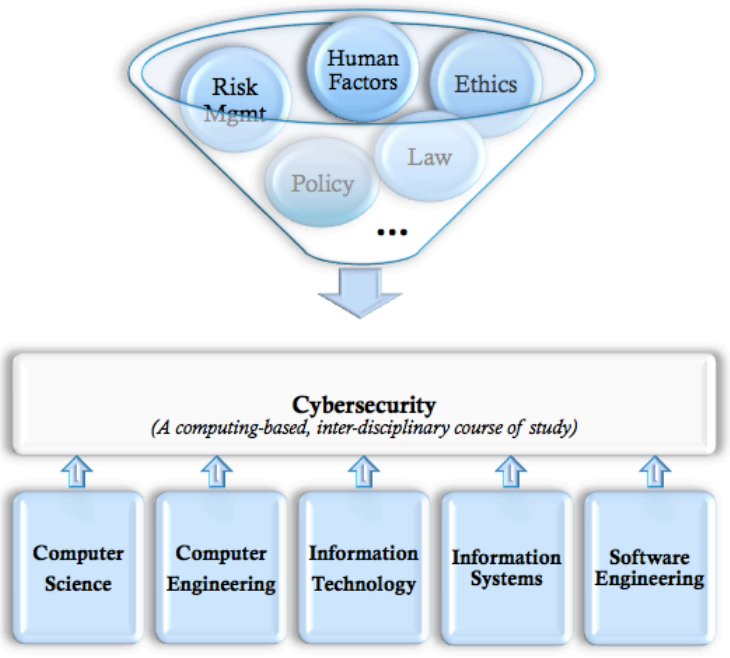
Early computing approaches relied on security that was built into the physical environment of the data center that housed the computers. As networked computers became the dominant style of computing, the ability to physically secure a networked computer was lost, and the stored information became more exposed to security threats. Larger organizations began integrating security into their computing strategies. Antivirus products became extremely popular, and cybersecurity began to emerge as an independent discipline.

The Internet brings millions of unsecured computer networks and billions of computer systems into continuous communication with each other. The security of each computer's stored information is contingent on the security level of every other computer to which it

is connected. Recent years have seen a growing awareness of the need to improve cybersecurity, as well as a realization that cybersecurity is important to national defense. The growing threat of cyber attacks has made governments and companies more aware of the need to defend the computerized control systems of utilities and other critical infrastructure. Another growing concern is the threat of nation-states engaging in information warfare, and the possibility that business and personal information systems could become casualties if they are undefended.

2.1 The Emergence of Cybersecurity as a Discipline

Cybersecurity is emerging as an identifiable discipline. It is perceived by most in the information technology industry as a field whose breadth and depth of content encompasses many of the sub-fields (e.g. software development, networking, database management) that form the modern computing ecosystem. The emergence of the discipline of cybersecurity is driven by the need for a computing discipline that can prepare specialists for the complexities and specific understanding of those complexities required to assure secure operation of cybernetic systems. It involves the creation, operation, analysis, and testing of secure computer systems. While cybersecurity is an interdisciplinary course of study; including aspects of law, policy, human factors, ethics, and risk management; it is fundamentally a computing-based discipline. As such, and as depicted below, academic programs in cybersecurity are both informed by the inter-disciplinary content, and driven by the needs and perspectives of the computing discipline that forms the programmatic foundation.



Cybersecurity as an identifiable degree field is still in its infancy. Driven by significant workforce needs, global academic institutions are developing a range of educational programs in the field. The curricular recommendations provided in this volume are framed by the computing disciplines: computer science, computer engineering, information technology, information systems, and software engineering.

2.2 Characteristics of a Cybersecurity Program

Each graduate of a cybersecurity program of study should have a cybersecurity curriculum that includes: (1) a computing-based (e.g. computer science, information technology) foundation; (2) cross-cutting concepts that are broadly applicable across the range of cybersecurity specializations (e.g. cybersecurity's inherent adversarial mindset); (3) a body of knowledge containing core cybersecurity knowledge and skills; (4) a direct relationship to the range of specializations meeting the in-demand domains (for reference, we use the domains identified in the US National Cybersecurity Workforce Framework[11]); and (5) a strong emphasis on the ethical responsibilities associated with the field. The curricular framework advanced in this volume will help academic institutions develop cybersecurity programs that meet each of these criteria.

[11]US National Cybersecurity Workforce Framework website: http://csrc.nist.gov/nice/framework/

Chapter 3: Cybersecurity Curricular Framework

Cybersecurity programs require curricular content that includes: (1) the theoretical and conceptual knowledge essential to understanding the discipline and; (2) opportunities to develop the practical skills that will support the application of that knowledge. The content included in any cybersecurity program is requires a delicate balance of breadth, depth, along with an alignment to workforce needs. It also demands a structure that simultaneously provides for consistency across programs of similar types while allowing for flexibility necessitated by both local needs and advancements in the body of knowledge. The curricular framework presented in the chapter supports the achievement of these goals.

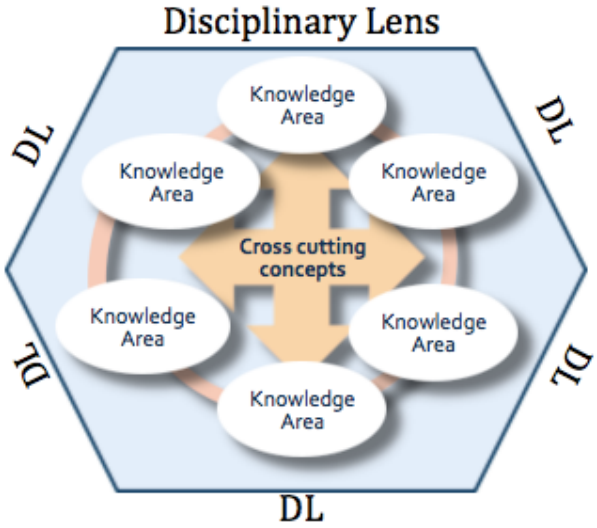
3.1 Philosophy and Approach

The CSEC2017 thought model is based on a rigorous review of existing curricular frameworks in science education, computing education, and cybersecurity education. Our philosophy, shaped in part by the U.S. National Research Council Next Generation Science Standards[12], views cybersecurity as a body of knowledge grounded in enduring principles and continuously extended, refined, and revised through evidence-based practice.

3.2 CSEC2017 Thought Model

The CSEC2017 thought model has four dimensions: knowledge areas, crosscutting concepts, disciplinary lens, and application areas. The depiction below shows the first three dimensions. The internal coloring of the model represents the presence of foundational knowledge. While not explicitly identified as a model dimension, foundational knowledge underlies and supports all of the curricular content described below. The fourth dimension, application areas, is used to link the curricular content to workforce frameworks and is described in a subsequent chapter.

[12] US National Research Council Next Generation Science Standards website: http://nextgenscience.org



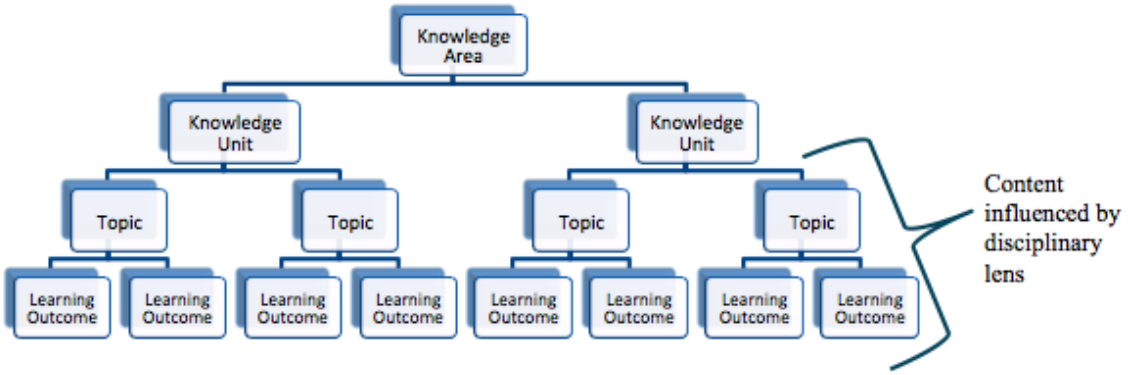
3.2.1 Foundational Knowledge

Students embarking on a cybersecurity course of study are expected to have a basic level of proficiency in foundational concepts. General education requirements provide an opportunity for students to learn basic communication, computational, and analytical skills. Other, more specialized foundational knowledge – fundamentals of information assurance, for example; should be introduced early and reinforced throughout the cybersecurity program. In the thought model, foundational knowledge sits outside of any single knowledge area and is depicted in the graphic by the colored space underlying the knowledge areas and crosscutting concepts.

3.2.2 Knowledge Areas

Knowledge areas serve as the basic organizing structure for cybersecurity content. Knowledge areas contain knowledge units - critical knowledge with broad importance within and across multiple computing-based disciplines. Collectively, knowledge areas represent the full body of knowledge within the field of cybersecurity.

The knowledge areas are structured as flexible buckets in the thought model to allow for the expansion and contraction of content as needed. Knowledge area content is structured with knowledge units - thematic groupings that encompass multiple, related topics; topics - curricular content; and learning outcomes - a description of what students should know or be able to do at the end of each topic. As shown below, each knowledge unit contains multiple topics and learning outcomes.



In the CSEC2017 thought model, each knowledge unit meets the following criteria:

- Has broad *(though variable, based on the disciplinary lens)* importance across multiple computing-based disciplines;
- Provides a key tool for understanding or investigating complex cybersecurity ideas; and
- Is both teachable and learnable over time and at increasing levels of depth and sophistication.

The disciplinary lens is used to focus the curricular content within each knowledge unit. It drives the depth and breadth of content covered in each topic, along with the associated learning outcomes.

The CSEC2017 thought model has six knowledge areas: data security, software security, system security, human security, organizational security, and societal security. The knowledge areas are organized by entities to be protected: data, software, systems, individuals, organizations, and society. The first three areas are primarily technical in nature while the last three areas include many topics not commonly taught in computing and engineering programs but with significant relevance to cybersecurity.

While the primary emphasis of each knowledge area is on protection and maintenance of security properties, some programs may choose to include the study of tools and techniques for circumventing protection mechanisms such as penetration testing. Due to the adversarial nature of cybersecurity, the study of "offensive" or "hacking" techniques is often a good way to develop stronger "defensive" cyber skills. All six of the knowledge areas include knowledge units that can be taught from both cyber defense and cyber offense perspectives. With that in mind, all cybersecurity programs should include coverage of ethics and cyber law across each of the knowledge areas.

Some cybersecurity programs may focus more heavily on the technical topics while others may include more emphasis on the individual, organizational and societal topics. However, the JTF believes that graduates of undergraduate cybersecurity programs

should study topics in all six areas. The knowledge areas are listed and described briefly below from the most narrowly focused to the most broadly focused.

- The **Data Security** area focuses on the protection of data at rest and in transit. This is the most narrowly focused and theoretical of the six areas, requiring the application of mathematical and analytical algorithms to fully implement. The primary goals of data security are to achieve confidentiality of information and preserve data and origin integrity. Knowledge units in this area include: cryptography, confidentiality, and data integrity.

- The **Software Security** area focuses on the development and use of software that reliably preserve the security properties of the information and systems they protect. This is the most specialized of the six knowledge areas and the least likely to be developed in depth by all cybersecurity programs. Knowledge units in this area include: high assurance software, secure software development, deployment, and maintenance, software reverse engineering, and malware analysis. An understanding of data security is important for many aspects of software security.

- The **System Security** area focuses on establishing and maintaining the security properties of systems, including those of interconnected components. The components include data, software, and hardware devices of all kinds, networks, and humans. Knowledge units in this broad area include: availability, authentication, access control, secure system design, reverse engineering, cyber physical systems, digital forensics, supply chain management, and computer network defense

- The **Human Security** area focuses on protecting individuals' personal data, their privacy and threat mitigation. It also includes the study of human behavior as it relates to cybersecurity. Knowledge units in this area include: identity management, social engineering, privacy, and security on social networks.

- The **Organizational Security** area focuses on protecting organizations from cybersecurity threats and on managing risk to support the successful accomplishment of the organization's mission. The organizations may be public or private, large or small, local, regional or international. Knowledge units in this area include: risk management, mission assurance, disaster recovery, business continuity, security evaluations and compliance, organizational behavior as it relates to cybersecurity, employee training, and intelligence.

  The **Societal Security** area focuses on aspects of cybersecurity that can broadly impact society as a whole for better or for worse. Knowledge units in this area include: cybercrime, cyber law, ethics, policy, intellectual property, professional responsibility, social responsibility, and cultural and international considerations

Some knowledge units will have relevance to, and could be logically placed in, multiple knowledge areas. This organization minimizes the overlap and provides a coherent organizational concept. Since knowledge units do not necessarily correspond to courses or course units, cybersecurity courses will typically contain topics from multiple knowledge units. Therefore placement of a knowledge unit under one knowledge area should not preclude its coverage in other knowledge areas.

3.2.3 Crosscutting Concepts

Crosscutting concepts help students explore connections among the core ideas, and are fundamental to an individual's ability to understand the core ideas regardless of the disciplinary lens. These concepts *"provide an organizational schema for interrelating knowledge*[13]*"* into a coherent view of cybersecurity. Each of the crosscutting concepts described below span most, if not all, of the knowledge areas.

The CSEC2017 thought model includes five crosscutting concepts: Confidentiality, Integrity, Availability, Risk, and Adversarial Thinking. The cross cutting concepts are described as follows:

- **Confidentiality**: rules that limit access to system information to unauthorized persons
- **Integrity**: assurance that information is accurate and trustworthy
- **Availability**: information is accessible
- **Risk**: exposure to environmental threats
- **Adversarial Thinking**: a thinking process that considers the potential actions of the opposing force working against the desired result

3.2.4 Disciplinary Lens

The disciplinary lens is the third dimension of the thought model. It represents the underlying computing discipline that forms the foundation of the cybersecurity program. As such, the disciplinary lens drives the approach, depth of content, and learning outcomes for each knowledge unit. It also influences the learning outcomes resulting from the interplay between the knowledge units and the crosscutting concepts.

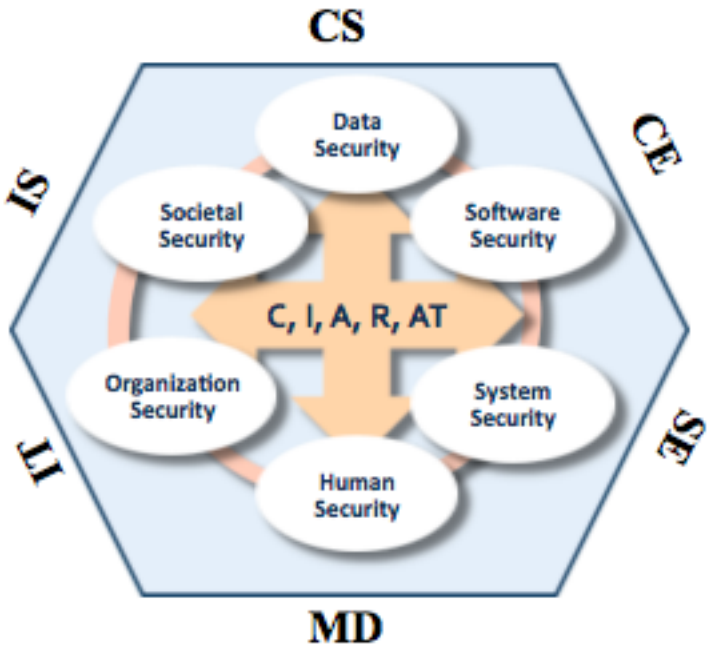
The CSEC2017 thought model encompasses the five computing disciplines identified by the ACM: computer science, computer engineering, information systems, information technology, software engineering, and a category for mixed or cross disciplinary majors established as "informatics" or "computational" programs.

[13] US National Research Council Next Generation Science Standards

The application of the crosscutting concept and/or the level of depth taught within each knowledge unit may differ depending upon the disciplinary lens. For instance, coverage of **Risk** in the context of **Data Security** may differ for students in a computer science cybersecurity program versus those in an information systems cybersecurity program.

3.2.5 Summary of CSEC2017 Thought Model

The dimensions of the thought model are depicted below:



- Foundational knowledge: general education and specialized cybersecurity foundations
- Knowledge areas: Data security, Software Security, System Security, Human Security, Organizational Security, and Societal Security
- Cross cutting concepts: Confidentiality, Integrity, Availability, Risk, and Adversarial Thinking
- Disciplinary lenses: Computer Science (CS); Computer Engineering (CE); Software Engineering (SE); Information Technology (IT); Information Systems (IS); and Mixed Disciplinary majors (MD)

Taken together, the combination of the dimensions provides a pathway to identify core content for learners in a range of computing-based cybersecurity programs. The application areas, described in chapter 6 of this volume, link the thought model to

workforce frameworks and provide insight for connecting curricular content and career development.

Chapter 4: Curricular Content

The curricular content (knowledge units and topics) was gathered and synthesized from a variety of sources including (in no particular order): ACM CS2013; ACM IT2017; US National Security Agency Centers of Academic Excellence; $(ISC)^2$; workforce frameworks such as the US National Initiative for Cybersecurity Education National Cybersecurity Workforce Framework (NICE NCFW), UK Government Communications Headquarters (GCHQ), and Skills Framework for the Information Age (SFIA); course exemplars sponsored by the Intel University Programs Office, the US National Science Foundation, and industry sector working groups; and other sources provided by the stakeholder community.

4.1 Foundational Knowledge

Recommendations for the foundational knowledge are categorized into general education and specialized cybersecurity foundations, and will be listed below.

4.2 Knowledge Areas

The tables below provide an overview of the curricular content for foundations and each knowledge area. For each knowledge area, the table lists knowledge units and the topics within each knowledge unit. Once the knowledge units and topics are refined, subsequent versions of this report will include specific learning outcomes and a recommended number of hours for each knowledge unit. Recommendations will be based on the disciplinary lens that is driving the curricular emphasis of each cybersecurity program. To assist in the process, the JTF will be convening disciplinary working groups for the five primary computing disciplines. The JTF welcomes comments on the current work and advance thoughts on the pending additions through the feedback form located at http://csec2017.org.

4.2.1 Knowledge Area: Data Security

The Data Security area focuses on the protection of data at rest and in transit. This is the most narrowly focused and theoretical of the six areas, requiring the application of mathematical and analytical algorithms to fully implement. The following table lists the knowledge units and component topics of the Data Security Knowledge Area.

Knowledge Unit	Topics
Information Security Fundamentals	Threats and Adversaries
	Vulnerabilities and Risk Assessment
	Intro to Cryptography

	Intro to Data Security (in transmission, at rest, in processing)
	Security Models
	Access Control Models (MAC, DAC, RBAC)
	Security Mechanisms (e.g., Identification/Authentication, Audit)
Cryptography	Symmetric Cryptography (DES, Twofish)
	Public Key Cryptography
	*Hash Functions (MD4, MD5, SHA-1, SHA-2, SHA-3) – for integrity, authentication, collision resistance
	Digital Signatures (Authentication)
	Key Management (creation, exchange/distribution)
	Cryptographic Modes (and their strengths and weaknesses)
	Types of Attacks (brute force, chosen plaintext, known plaintext, differential and linear cryptanalysis, etc.)
	Common Cryptographic Protocols
	Evolution of Algorithms (DES to AES etc.)
	Security Functions (data protection, data integrity, authentication)
	Number Theory
	Probability and Statistics
	Understanding of the major algorithms (AES, RSA, EC)
	Suite B Algorithms
	Understanding of the families of attacks (differential, man-in-the-middle, linear, etc.)
	Hashing and Signatures
	Key Management
	Modes and appropriate uses
	Classical Cryptanalysis (a la Konheim)
	Identity-based Cryptography
	Digital Signatures
	Virtual Private Networks
	Quantum Key Cryptography

4.2.2 Knowledge Area: Software Security

The Software Security area focuses on the development and use of software that reliably preserve the security properties of the information and systems they protect. This is the most specialized of the six knowledge areas and the least likely to be developed in depth by all cybersecurity programs. The following table lists the knowledge units and component topics of the Software Security Knowledge Area.

1

Knowledge Unit	Topics
Fundamental Design Principles	Separation (of domains)
	Isolation
	Encapsulation
	Least Privilege
	Simplicity (of design)
	Minimization (of implementation)
	Fail Safe Defaults Fail Secure
	Modularity
	Layering
	Least Astonishment
	Open Design
	Usability
	End-to-End Security
	Defense in Depth
Practice	Specification of Security Requirements
	Principles of Secure Programming
	Robust/Defensive Programming
	Input Validation, Sanitization
	Type Checking and Coercion
	Overflows (buffer, integer, other)
	Race conditions
	Validating Environment
	Programming Flaws
	Static, Dynamic Analysis
	Data Obfuscation
	Protecting sensitive data
	Software Development Life Cycle
	Software testing
	Penetration testing Fuzz testing
	Choice of Programming Language and Type-Safe Languages
	Injections (SQL, command, etc.)
	Cross-site Scripting
	Exception Handling
	Error Handling
	Randomness
Documentation	Documentation

2

4.2.3 Knowledge Area: System Security

The System Security area focuses on establishing and maintaining the security properties of systems, including those of interconnected components. The components include data, software, hardware devices, networks, and humans. The following table lists the knowledge units and component topics of the System Security Knowledge Area.

Knowledge Unit	Topic
Availability	System availability
	Measures of availability
	Attacks on availability
Authentication	Passwords and PINs
	Keys, cards, certificates
	Biometric authentication
	Multifactor authentication
	Authentication protocols
	Machine authentication`
Access Controls	Security policies
	Access control models
	Access control implementation
	Account management
	System audit
Secure Systems Design	Security Design Principles
	Security Architectures
	Trusted Computing Base
	Security Modes of Operation
Computer Network Defense	Threats and Vulnerabilities
	Host-based protection
	Firewalls
	Intrusion Detection and Intrusion Prevention Systems
	Honeypots
Reverse Engineering	Disassembly techniques
	Anti-tamper techniques
	Fuzzing
	Reverse Engineering Tools
Cyber Physical Systems *Security*	Industrial Control Systems
	Internet of Things
	Threats and vulnerabilities
Digital Forensics	Rules of Evidence
	Preservation of Data

	OS/File System Forensics
	Application Forensics
	Network Forensics
	Mobile Device Forensics

4.2.4 Knowledge Area: Human Security

The Human Security area focuses on protecting individuals' personal data, their privacy and threat mitigation. It also includes the study of human behavior as it relates to cybersecurity. The following table lists the knowledge units and component topics of the Human Security Knowledge Area.

Knowledge Unit	**Topic**
Identity Management	
	Physical and logical assets control
	Identification and authentication of people and devices
	Identity as a service (e.g. cloud identity)
	Third-party identity services (e.g. on-premise)
	Access control attacks
	Identity and access provisioning lifecycle (e.g. provisioning review)
Social Engineering	
	Attacks on privacy and anonymity
	Privacy policy
Social Networks	
	Social Networking Technologies
	Social Networking Concepts
	Successful social networks
Human Computer Interaction	Human Factors
Fundamental Security Design Principles	
	Separation (of domains)
	Isolation
	Encapsulation
	Least Privilege
	Simplicity (of design)
	Minimization (of implementation)

	Fail Safe Defaults / Fail Secure
	Modularity
	Layering
	Least Astonishment
	Open Design
	Usability

4.2.5 Knowledge Area: Organizational Security

The Organizational Security area focuses on protecting organizations from cybersecurity threats and on managing risk to support the successful accomplishment of the organization's mission. The following table lists the knowledge units and component topics of the Organizational Security Knowledge Area.

Knowledge Unit	**Topics**
Security Policy and Governance	
	Privacy
	Organizational policies – (e.g. breach disclosure, data retention)
	Legal, Ethics and Compliance
	Organizational Context
	Business Continuity / Disaster Recovery
	Reporting requirements
Analytical Tools	
	Security metrics
	Data analysis and Interpretation
	Probability and Statistics
Systems Administration	
Cybersecurity Planning	
	Operational and tactical management
	Executive and board level communication
	Strategic planning
Security Program Management	
	Project management
	Resource management
	Quality Assurance / Quality Control
	Supply chain security
Security Awareness, Training and Education	
Risk Management	
	Risk Assessment and Analysis

	Risk Measurement and Evaluation Methodologies	1
	Risk Management Models	2
	Risk Management Processes	
	Mitigation	
	Communication of Risk	

4.2.6 Knowledge Area: Societal Security

The Societal Security area focuses on aspects of cybersecurity that can broadly impact society as a whole for better or for worse. The following table lists the knowledge units and component topics of the Societal Security Knowledge Area.

Knowledge Unit	Topics
Cybercrime	Cyber Criminal Behavior
	Cyber Terrorism
	Cyber Criminal Investigations
	Digital Evidence: Chain of Custody
	Cyber-focused crimes
	Cyber-assisted crimes
	Economics of Cybercrime
	Dark Web
Cyber law	Constitutional Foundations of Cyber Law
	Military and civilian cyber law
	Intellectual property
	Digital Evidence: Digital Forensics
	Privacy Laws
	Data security law
	Computer hacking laws
	Digital contracts
Ethics	Cyber ethical frameworks
	Cyber normative theories
	Professional ethics and codes of conduct
Policy	Cyber War and Strategy
	International Cyber Laws and Policy
	U.S. Cyber Policy
Privacy	Privacy norms
Intellectual Property	Intellectual property and cybersecurity
Professional Responsibility	Professional responsibility for cyber professionals
Social Responsibility	Ethical hacking
Global Impacts	Internet governance

4.3 Recommended Hours per Knowledge Area

The next version of the CSEC2017 report will provide initial recommendations, along with the rationale, for the number of hours for each knowledge area by knowledge unit and disciplinary lens. The recommended hours will be provided by discipline and in summary form using a table structured as follows:

KA: Data Security	DL CS	DL CE	DL SE	DL IT	DL IS
KU 1					
Topic 1					
Topic 2					
…					
KU 2					
Topic 1					
Topic 2					
…					
KU 3					
…					
…					
…					
Total					

Cybersecurity experts wishing to participate in the disciplinary working groups are encouraged to provide feedback on knowledge units and topics included in this report, and to express their interest through the feedback form located at http://csec2017.org.

4.4 Course Guidance

Because curricular content can be distributed throughout the curriculum in a number of ways, this document does not provide specific guidance on courses. Rather, the CSEC2017 report will provide recommendations on the number of hours per topic within the context of each discipline. This structure allows for maximum flexibility as academic institutions seeks to develop programs within their specific environments. However, academic institutions seeking specific course guidance are encouraged to review the program exemplars, which will be included in the appendix of the final report. Institutions or individuals wishing to discuss how their programs and courses might be included as exemplars are encouraged to provide feedback on this report and to express their interest through the feedback form located at http://csec2017.org.

4.5 Learning Outcome Guidance

Learning outcomes describe what a student should know or be able to do at the conclusion of each topic. The learning outcome guidance to be included in the CSEC2017 report will follow the definition and structure of the CS2013 report by defining three levels of mastery:

- Conceptualization: The learner understands the essence of the concept and has an awareness of its meaning. This learning outcome answers the question "What do you know about this?"
- Application: The learner is able to use or apply a concept. This learning outcome answers the question "What do you know how to do?"
- Interpretation: The learner is able to apply the concept in multiple contexts, select an appropriate approach from understood alternatives, and consider a concept from multiple viewpoints. The learning outcome answers the question "Why would you do that?"

The next version of the CSEC2017 report will provide initial recommendations, along with the rationale, for the learning outcomes associated with each topic.

Chapter 5: Industry Perspectives on Cybersecurity

The field of cybersecurity is in the formative stages of development and is experiencing growing pains as the need for the discipline is recognized throughout industry. While the discipline has grown in past decades, cybersecurity has been frequently discounted or overlooked as a critical success factor across business, industry, government, services, organizations, and other structured entities that use computers to automate or drive their products or services efficiently. There is a growing consensus that this must change.

People seeking careers in cybersecurity have a great potential for success. Findings from the International Information Systems Security Certification Consortium $(ISC)^2$ workforce survey predict that by 2020 there will be a global shortage of 1.5 Million cybersecurity professionals (National Institute of Standards and Technology / National Initiative for Cybersecurity Education (NIST/NICE) Workforce Demand Report, 2015). Unfortunately, although jobs are and will be available, finding qualified people to fill them is often difficult. Students graduating from technical programs such as information technology often do not have the attributes to fill the needs of industry. Perhaps they have technical skills acquired from their studies, but they lack other skills needed "to fit" within an industry or government environment.

5.1 The Academic Myth

Students who graduate from a four-year university program assume that the baccalaureate degree is a sufficient qualification to attain a position. This understanding may be true in some fields, but not necessarily in the computing disciplines nor specifically in cybersecurity. Belief in this myth has stymied many a job hunter worldwide. The degree credential is growing in importance, but it is not a sufficient condition for a position. A general understanding exists in cybersecurity and other fields that a successful professional must be a good communicator, a strong team player, and a person with passion to succeed. Hence, having a degree is not sufficient to secure employment.

Some people believe that a graduate of an cybersecurity program who has a high grade-point-average (GPA) is more likely to attain a position than one who has a lower GPA. This is another mythical belief. A graduate having a high GPA is commendable. However, if s/he does not have the passion and drive, does not work well in teams, and does not communicate effectively, chances are that the person will not pass the first interview.

5.2 Non-technical Skills

Non-technical (sometimes called "soft") skills are vital to the success of cybersecurity professionals. The ability to work in a team, communicate technical topics to non-technical audiences, successfully argue for resource allocations, hone situational awareness, and operate within disparate organizational cultures are just a few of these skills. The US Chief Human Capital Officers Council (CHCO), among other bodies, has

developed a list of non-technical competencies pertinent to the cybersecurity workforce. The list includes: accountability, attention to detail, resilience, conflict management, reasoning, verbal and written communication, and teamwork. The full list of competencies is available in the Competency Model for Cybersecurity[14]. Professional associations such as (ISC)[2] and ISACA also provide recommendations for non-technical skills required for cybersecurity professionals.

5.3 The Technical - Business Skills Continuum

Many of the solutions to the cybersecurity problem are technical, but they also require that individuals and organizations implement policy and program activities to make intended control systems function properly. There does exist a continuum of skillsets within the discipline of cybersecurity ranging from the highly technical (areas like cryptography and network defense) to the highly managerial (areas like planning, policy development and regulatory compliance). Regardless of where one is positioned within the cybersecurity workforce, each graduate of a cybersecurity program will need a combination of skills from areas across this broad continuum and should possess both the technical skills and the business acumen to effectively participate in the problem solving, analysis, and project management activities necessary to implement cybersecurity solutions.

5.4 Sector-based Industry Needs

Many contributors to this report have identified the critical need in meeting cybersecurity workforce needs for coming years both at their specific companies and in the broader business community. These sector specific needs will be explored further in subsequent versions of this report.

5.5 Career Focus

As students prepare for their future career, an important consideration is their ability to be able to transition from an academic environment to a career within a corporation, organization, academic institution, or even an entrepreneurial environment. One can appreciate what a difficult transition this can be if an individual has not received the proper mix of both technical and soft skills exposure during their academic career.

Adaptability is a personality trait that is especially important within the cybersecurity industry, and will be very important for career success in the future. We find that adaptability describes the ability "to adjust oneself readily to different conditions"[15]. Employees will find the ability to learn new technologies and embrace change to be of considerable importance in years to come. Georgia Nugent states, "It's a horrible irony that at the very moment the world has become more complex, we're encouraging our

[14] US Chief Human Capital Officers Council Competency Model for Cybersecurity https://www.chcoc.gov/content/competency-model-cybersecurity
[15] Reference: http://www.dictionary.com/browse/adaptable

young people to be highly specialized in one task. We are doing a disservice to young people by telling them that life is a straight path. The liberal arts are still relevant because they prepare students to be flexible and adaptable to changing circumstances"[16]. The cybersecurity industry has historically appealed to individuals who thrive in this environment of constant change.

In addition to focusing on the industry and gaining valuable work experience while attending a university, it is important that students nearing graduation are ready for important interviews by structuring their resumes into a format that highlights their technology background. What distinguishes a technical resume from a standard one is the emphasis on attributes such as specific technical skill sets and industry certifications. Monster.com, a leading job board and career site, is a good source for examples of how to create a technical resume[17].

Being able to handle a successful interview is a career skill that is essential for students to practice and master in the course of their academic studies. It is as important as learning basic technical subjects. If students are unable to handle the rigors of a career interview, their academic GPA and various scholastic achievements will fail them in achieving the desire goal of a useful cybersecurity education—to graduate and secure a position that can lead to career fulfillment and growth.

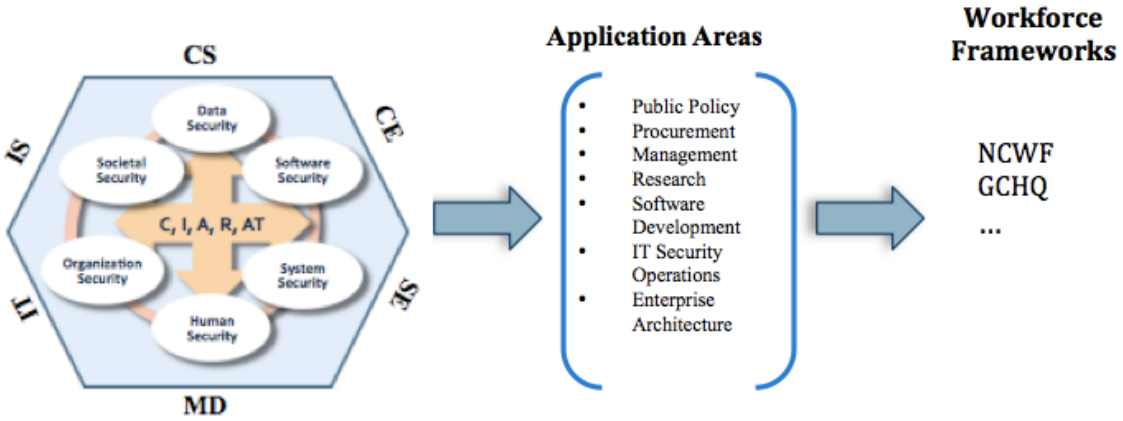
A cybersecurity advisory board can help academic programs provide students with important networking within the broader cybersecurity industry and the specific employment options in cybersecurity that will also help them to perform successfully in the interviewing process. Often, advisory boards act as mentors to students, giving them valuable feedback on their resumes and academic background. They will often aid and encourage students to work in internships, the value of which is also a topic for discussion. Additionally, the importance of non-technical skills and getting along in a team environment are all components of good networking. To continue and advance in one's career in the future, the ability to network and find career opportunities will become a very important skill.

[16] Reference: https://www.fastcompany.com/3034947/the-future-of-work/why-top-tech-ceos-want-employees-with-liberal-arts-degrees
[17] Monster.com website: http:/monster.com

Chapter 6: Linking Cybersecurity Curriculum to Professional Practice

Cybersecurity practices refer to the combination of knowledge and skills required to perform in the field. Practices are a critical consideration in cybersecurity education. The CSEC2017 thought model links the academic curriculum to professional practice through the use of application areas.

The application areas provide an organizing structure to combine curricular content, professional development and training opportunities, and professional certifications. In subsequent versions of the CSEC2017 report, the contents included in each application area will be fully explored.



6.1 Application Areas

Application areas serve as an organizing framework to identify competency levels for each practice. The application areas help to define the depth of coverage needed for each core idea. In addition, application areas provide a bridge between the thought model and a specific workforce framework

The seven application areas included are:

- Public Policy — Executive management (at the level of CEO or board of directors), legislators who will pass laws affecting the development, deployment, and use of information technology, regulators who will regulate those things, and other public and private officials will develop a *de facto* public policy. These people must understand how those laws, regulations, and requirements affect the use of the systems, how people interact with them and with the regulating authorities, how compliance checking is done, and what risks the public policy both controls and introduces. As the design of a system, and the process in which the organization uses it, affect the way compliance is implemented and tested,

they must understand the basics of design. This leads to the need to understand what a computing system can, and (perhaps more importantly) cannot, so. This also means they must understand the cost of security, in budgetary and human terms.

- Procurement — Those who procure information technology, and who hire the people who will work with it, must understand how the systems and the hires fit into the goals of the organization in general and the particular goals of the project(s) for which the procurement and hiring is undertaken. This requires an understanding both of business continuity and risk management, the latter so the technology and people are chosen to minimize risk, to make risk as easy as possible to manage, or (ideally) both. The implication of these is to know what is required of people, systems, infrastructure, procedures, and processes to provide the desired level and assurance of security.

- Management — Management refers to both systems and people within an organization of some type. Both internal policies and external policies (regulations, laws, etc.) affect management. Managers must understand compliance and business continuity issues in order to ensure the systems and people they manage meet the needs of the organization and governmental and other regulators. As they must ensure that people using their systems are authorized to, and know whom those people are, they must be well versed in identity and authorization management. Changes to the systems require that they understand the goals of testing and whether the manner in which the tests are conducted speak to those goals. Finally, they must be prepared to deal with the results of attacks, both by understanding how to manage the incidents and how the incident will affect the organization. Thus, they must have a basic understanding of both incident management and accident recovery.

- Research — Researchers in academia, industry, and government who study security should know the basics of access control, confidentiality (including the basic principles and use of cryptography), integrity, and availability. Beyond that, the specifics of what they should know depends upon their area of research, and any specific goals of that research. For example, a researcher studying network security should understand how the networks are used in practice in order to understand how their operation affects the parameters of her research; it is probably unnecessary to understand the proof of the HRU theorem and the associated results. But someone studying foundational aspects (such as undecidability) needs to know the HRU theorem and related results, and not the details of network operations.

- Software Development — Software must meet requirements, which are often controlled by laws, regulations, business plans, and organizational factors. Developers muse ensure their software is designed to meet these requirements, or the requirements are changes to what the software can satisfy. Then their implementations must satisfy the design and be robust (“secure programming”), which includes the proper handling of exceptions and errors. This includes taking into account the environment in which the software will operate. They must know

how to validate their claims by testing the software. Finally, they must be able to set the environment in which the software will run to that which their design and implementation assumes; and if this cannot be done, they must document this in their installation guides, and (ideally) display appropriate messages during the installation of the software.

- IT Security Operations — Similarly, operations must preserve the security of the system. As "security" is defined by a set of requirements, the system administrators, system security officers, and other information security personnel must understand how to translate requirements into procedures and configurations. They must be able to design and implement security enclaves and infrastructures to this end, for example ensure that identity and authorization management systems are installed, initialized, configured, and connected properly. They will need to know how to test the systems, infrastructure, and procedures, and analyze the results. Finally, the operations personnel must understand system maintenance under both normal conditions (patching and upgrading, for example) and abnormal conditions (incident handling and response, for example).

- Enterprise Architecture — Enterprise architecture refers to the systems, infrastructure, operations, and management of all information technology throughout an enterprise. This requires elements from all other applications areas. Policy drives the architecture; the design of the architecture drives procurement, management, and operations. The architecture also affects much of the software, for example that needed to run the infrastructure. Therefore, the enterprise architects must understand the policy, procurement, management and operations application areas, as well as elements from the area of software development.

6.2 Training and Certifications

In the field of cybersecurity, knowledge acquisition and skill development, even at the undergraduate level, occurs in both formal higher education settings and professional development training and certification space. The relationship between these educational settings, and recommendations for collaborative initiatives will be explored in subsequent versions of this report.

6.3 Workforce Frameworks

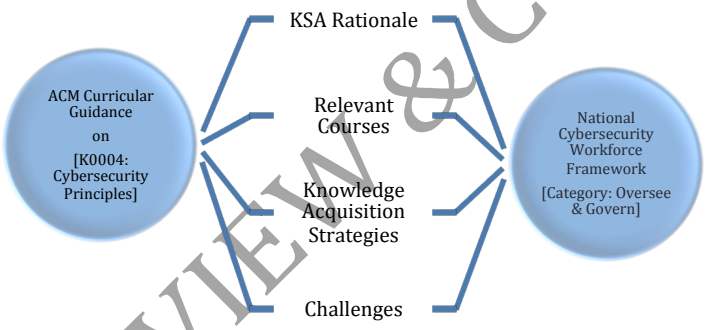
Workforce development initiatives are often driven by workforce frameworks that provide an organizing structure for the various job roles; education, training and professional development requirements; and career pathways; within the context of the larger economic environment. In the field of cybersecurity, nations have begun to develop workforce frameworks to outline skill requirements and support workforce development initiatives. In the US, the National Initiative for Cybersecurity Education

National Cybersecurity Workforce Framework (NCWF)[18] is being developed as a comprehensive resource to describe cybersecurity work.

6.4 NCWF Implementation Roadmaps

The final version of this report will provide course roadmap exemplars that describe a pathway for knowledge acquisition that links the ACM CSEC2017 Curricular Guidance to the National Cybersecurity Workforce Framework. The first exemplar will focus on linking the foundational KSA - *K0004: Knowledge of Cybersecurity Principles* as outlined in the NCWF to Work Roles within the *Oversee and Govern (OV)* category. Other roadmaps will be developed based on manpower and resource availability.

Each course roadmap will (a) provide a rationale for knowledge and its importance for the specific work role; (b) identify and describe relevant courses and course modules; (c) outline strategies for obtaining the knowledge when specific courses are not available or accessible within the institution; and (d) highlight challenges (and associated strategies to overcome them) to following the suggested course of study.



The above graphic shows how the roadmaps will link the curricular guidance and the workforce framework. Below, each roadmap element is described in greater detail.

6.4.1 KSA Rationale

The KSA rationale will provide a frame of reference for students embarking on the course of study. It will explain the relationship between the knowledge and the specific work role.

6.4.2 Relevant Courses

The central portion of the roadmap will be the identification of relevant courses and a description of needed course content. Because relevant courses are spread through the

[18] National Cybersecurity Workforce Framework: http://csrc.nist.gov/nice/framework/

university in a variety of schools and in a variety of formats, it will be critical to include specific content in this section, not simply a listing of course titles. This section of the roadmaps will also include strategies for independent study courses and other customizable options.

6.4.3 Knowledge Acquisition Strategies.

Universities have often have programs and courses housed across multiple university academic units. In addition, some relevant content may be accessible through activities that are external to the formal course structure. As a result, it can be challenging for students (and their faculty advisors) to identify the most effective knowledge acquisition strategies. The roadmaps will assist in this navigational effort.

6.4.4 Challenges

Roadmaps represent the ideal plan of study. However, implementing the roadmaps within the context of the university structure, even when that context has been explicitly considered in the development process, can be challenging. This section of the roadmaps will outline specific challenges and suggest strategies to overcome them.

Taken together, the four roadmap elements will provide a comprehensive planning document for both students and faculty members.

Chapter 7: Institutional Implementation

Chapter 7 will provide advice for institutions seeking to implement recommendations from the CSEC2017 curricular volume. The following sections will be discussed:

- Local adaptation and variations between institutional types
- Technical resource requirements (onsite facilities, virtual laboratory environments)
- Faculty recruitment and retention strategies
- Obtaining institutional support
- Broadening participation
- Maintaining curricular currency
- Leveraging local and regional resources

[End of CSEC2017 v. 0.5]

Public Review and Comment period: January 14 – February 14, 2017
Provide feedback at: http://csec2017.org

Page intentionally left blank

Appendix A: Contributors

Sherly Abraham, Georgia Gwinnett College
Joshua Adams, Saint Leo University
Sara Akers, Terra State Community College
Dr. Ankur Chattopadhyay, University of Wisconsin - Green Bay
Thibaud Antignac, Chalmers University of Technology
Alan B. Watkins, National University
A lbert Ball, Hodges University
Masooda Bashir, UIUC
Shannon Beasley, PhD, Middle Georgia State University
Kimberly Bertschy, Northwest Arkansas Community College
Diana Bidulescu, HISD
Chutima Boonthum-Denecke, Hampton University
Brandi Boucher Fabel, Ivy Tech Community College
Michael Brian Pope, Independent Scholar
Nelbert C. St.Clair, Middle Georgia State University
William (Bill) Caelli, QUT / GU
Roy Campbell, University of Illinois at Urbana-Champaign
Martin Carlisle, Carnegie Mellon University
John Chandy, University of Connecticut
Zhen Chen, Tsinghua University
Li-Chiou Chen, Pace University
Jessica Chisholm, Valencia College
KP Chow, Department of Computer Science, University of Hong Kong
Timothy Cullen,
Leslie D. Fife, PhD,
Kevin Daimi, University of Detroit Mercy
Ruth Davis, Santa Clara University
Bostjan Delak, ITAD
Ravi Dhungel, Intuit
Bill Doherty, Truckee Meadows Community College
L. Drevin, NWU
Alvaro E. Arenas, IE Business School
Burkhard Englert, CSULB
Dave Filer, New River Community College
Guillermo Francia, III, Jacksonville State University
Robert Francis, Federal Reserve Bank of New York
Dr. Lothar Fritsch, Karlstad University
Janos Fustos, MSU Denver
Thoshitha Gamage, Southern Illinois University Edwardsville
Jim Gast, ITT Tech
Dickie George, JHUAPL
Duane Gerstenberger , Marion Technical College
Joseph Giordano, Utica College
Bonnie Goins, Illinois Institute of Technology
Kartik Gopalan, Binghamton University
Andy Green, Kennesaw State University
Steve Hailey, CyberSecurity Academy
H. Hall, Athens Technical College

K Harisaiprasad, Manhindra
Jim Helm, ASU
Morgan Henrie, MH Consulting, Inc
Jayantha Herath, St. Cloud State University
Erik HjelmÃ¥s, NTNU
Adrianna Holden-Gouveia, Northern Essex Community College
Susan Holland, University of Massachusetts Lowell
Micaela Hoskins, Cisco Systems
Grant Hudson, United States Postal Service
Andrew Hurd, Excelsior College
John Impagliazzo, Hofstra University
Stephen Itoga, University of Hawaii at Manoa
Danis J. Heighton, Clark State Community College
Murray Jennex, San Diego State University
Sonja Johnson,
Thomas Kaczmarek, Marquette University
Chris Kadlec, Georgia Southern University
Andrew Kalafut, Grand Valley State University
Alan Katerinsky, Hilbert College
Jonathan Katz, University of Maryland
Walter Kerner, Fashion Institute of Technology Rami Khasawneh, Ph.D., Lewis University
Valentin Kisimov, UNWE Bulgaria
Donald Kraft, Colorado Technical University and U.S. Air Force Academy
Ojoung Kwon, California State University at Fresno
Angel L Hueca, Nova Southeastern University
David Lanter, Temple University
Stephen Larson, Slippery Rock University of PA
Margaret Leary, Northern Virginia Community College
Roy Levow, Florida Atlantic University
Peng Li, East Carolina University
Xun Luo, China Computer Federation
Qutaibah Malluhi, Qatar University
Fabio Massacci, University of Trento
Nancy Mead, Carnegie Mellon University
Mark Merkow, Charles Schwab and Co., Inc.
Dr. Michael Whitman, Kennesaw State University
NG MIEN TA, Wizlearn Technologies Pte Ltd
Dustin Mink, University of West Florida
Michael Moorman, Saint Leo University
Mike Murphy, retired
Lillian N Cassel, Villanova University
James N. Smith, Nova Southeastern University
Robert Olson, Rochester Institute of Technology
Jacques Ophoff, University of Cape Town
Bernardo Palazzi, Brown University
Hyungbae Park, University of Central Missouri
Malcolm Pattinson, University of Adelaide
Kimberly Perez, Tidewater Community College
Mathew "Pete" Peterson,
Amelia Phillips, Highline College
Joe Pilla, Liberty Tax

Christine Pommerening, George Mason University
Damira Pon, University at Albany, State University of New York
Dr. Priyadarsi Nanda, University of Technology Sydney, Australia;
Dr. Mathias R. Plass, Lewis University;
Alan Rea, Western Michigan University
Thomas Reddington, New York Univesity (NYU)
Randy Reid, UWF
Andrew Rozema, Grand Rapids Community College
Gerry Santoro, Penn State University
Gordon Shenkle, Industry
Dan Shoemaker, Center for Cybersecurity University of Detroit Mercy
Neelu Sinha, Fairleigh Dickinson University
Jill Slay, UNSW Canberra
S Srinivasan, Texas Southern University
Mark Stockman, University of Cincinnati
S M Taiabul Haque, University of Central Missouri
April Tanner, Jackson State University
David Tobey, Indiana University South Bend
Kim Tracy, Michigan Technological University
Ray Trygstad, Illinois Institute of Technology
Michael Tu, Purdue University Northwest
Douglas Twitchell, Boise State University
Randal Vaughn, Baylor University
Harald Vranken, Open University of the Netherlands
Paul Wagner, University of Wisconsin - Eau Claire
James Walden, Northern Kentucky University
Charles Walker, Federal Govt
David Wang, DePaul University
Xinli Wang, Michigan Technological University
Deanne Wesley, Forsyth Technical Community College
Doug White, Roger Williams University
Patrea Wilson, University of Maryland University College
Scott Woodison, Univ system of Georgia (Ret)
Carol Woody, Software Engineering Institute
Xiaodong Yue, University of Central Missouri
Neal Ziring, NSA
Kenneth Hoganson

Page intentionally left blank