Toward Curricular Guidelines for Cybersecurity

Report of a Workshop on Cybersecurity Education and Training

Andrew McGettrick
Professor, University of Strathclyde
Chair, Education Board
Association for Computing Machinery (ACM)

August 30, 2013

Work supported by the National Science Foundation

Executive Summary

The *Cyberspace Policy Review*, published in 2009, argued for a national strategy to develop a cybersecurity workforce adequate in numbers and expertise to secure the United States in cyberspace. In assessing education and training, the Review said, "Existing cybersecurity training and personnel development programs, while good, are limited in focus and lack unity of effort. In order to effectively ensure our continued technical advantage and future cybersecurity, we must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees."[1] A number of workshops and a wide range of initiatives have occurred in recent years to help develop a comprehensive and coordinated plan to build a cybersecurity workforce adequate to meet the pressing needs of business and government.

A Core Leadership Group comprising cybersecurity experts in government, industry, and academia gathered in Atlanta 21-22 February 2013 to discuss current cybersecurity education initiatives and make recommendations that will inform near-term and long-range curricular guidance in cybersecurity for colleges and universities. The group also discussed the roles for government and private industry to play in building a broad cybersecurity workforce ranging from proficient technicians and practitioners to policy makers and thought leaders.

Workshop participants embraced the philosophy expressed by ACM's policy arm (USACM) and the Computing Research Association (CRA) that computer science and computer engineering graduates should possess a thorough **education** in cybersecurity and related fundamentals and principles as well as **training** in cybersecurity-specific technologies, tools, and skills. The balance between education and training may vary for particular knowledge areas or sub-specialties, but a strong underpinning of basic knowledge and principles to complement technical skills should form the basis of a curriculum in cybersecurity.

The leadership group offered perspectives on the educational components that should be incorporated into traditional degree programs.

Doctoral degrees support next-generation cybersecurity education and research in academia, and provide thought leadership and advanced expertise necessary for industry and government. Our best and brightest have much to contribute:

- Ability to think, set, and achieve long-term research goals
- Ability to apply theoretical foundations of cybersecurity to real-world challenges
- Ability to combine theoretical and practical understanding to inform cybersecurity policies and assess innovations
- Ability to mentor the next generation of students and potential leaders
- Willingness to seek career aspirations both within and outside academia

Currently, few PhDs in information assurance and cybersecurity return to academia to educate future generations.[2] We need a vibrant mechanism to create PhDs in cybersecurity. An important step in that direction would be to better leverage the Department of Homeland Security (DHS)/National Security Agency (NSA) Information Assurance Scholarship Program, designed to assist in recruiting and retaining highly qualified personnel to meet the Department of Defense's (DoD) information technology requirements for national defense and the security of its information infrastructure; as well as NSF's investment in the CyberCorps® Scholarship for Services (SFS) to allow SFS-funded graduates with advanced degrees to serve their government service requirement in academia where they can help to enhance the security component of existing courses, develop new ones, and contribute to faculty professional development.

Master's degrees are essential for providing a cybersecurity workforce with advanced capabilities. Building on a sound baccalaureate degree in computer science or related area, an additional two years of education could cover important technical cybersecurity topics. A master's degree in cybersecurity in a two-year timeframe would allow suitably prepared graduates to master the knowledge, skills, and abilities (KSAs) specific to advanced topics in cybersecurity.

Universities should provide several master's degree options addressing cybersecurity issues:

a. **Cybersecurity for computing professionals**--Strongly technical cybersecurity-specific degree programs focusing on cybersecurity built upon a rigorous undergraduate background in computer engineering, computer science, or software engineering
b. **Cybersecurity in society**--Master's programs in non-computing disciplines that emphasize cybersecurity challenges and vulnerabilities and their implications for various professions, including law, business, economics, and medicine
c. **Cybersecurity operations**—Practical techniques and technologies for recognizing vulnerabilities and preventing security breaches

Business and government could encourage and improve cyber expertise by funding scholarships to help students afford graduate-level courses in cybersecurity.

Associate degrees in computing disciplines focus on graduating a technically proficient and employable workforce in a relatively compressed timeframe. They help to feed technically-adept practitioners into the cybersecurity workforce pipeline. Two-year colleges are doing an excellent job in addressing cybersecurity education at the college level, graduating students directly into the workforce as well as transferring students into baccalaureate degree programs. Community colleges and other two-year institutions tend to coordinate their curricula with KSAs needed by local businesses. The community of cybersecurity stakeholders, particularly government and private industry, should generously fund and support community colleges in their efforts.

Undergraduate baccalaureate degrees present serious challenges to enhancing cybersecurity education because to some extent adding knowledge areas at the baccalaureate level is a zero-sum game. The curriculum for any computing major already has tight time allotments, and "elbowing in" cybersecurity knowledge areas must be done carefully so as not to "elbow out" topics deemed essential in the curriculum.

Workshop participants offered suggestions that educational institutions should consider when weaving cybersecurity topics into undergraduate curricula.

For all undergraduates:

- At all levels, there is a need for understanding and practicing cybersecurity in a human context, taking into consideration workflow, human nature, and other practical constraints. A recent report[3] recommends adopting a doctrine of public cybersecurity that envisions cybersecurity as a public good. In this view, governmental bodies with the authority to make and enforce public policy would set standards and regulate cybersecurity activities in the same way that public health institutions such as the NIH currently promulgate health policies and practices. Educational institutions have a vital role to play in raising the security awareness of citizens and influencing their security behavior.

- Many disciplines (law, medicine, business, international studies, publishing, and many more) have related cybersecurity issues that should be part of each student's curriculum. Indeed, awareness of the principles and challenges of information security and privacy

should be woven into the entire curriculum, though finding or training faculty members to add this dimension could well be challenging.

For computing majors:

- Each student in a computing-related degree program should be required to take at least one technical course in a security-related knowledge area.

- Faculty should exemplify to students a responsible attitude toward security issues.

- Faculty with a low comfort level in teaching security topics are prone to give security topics inadequate attention. Faculty members should gain competence and confidence to teach cybersecurity in its many contexts, or be willing to have colleagues with that expertise collaborate with them on teaching security topics.

- Where appropriate, institutions should create credentials or certificates in security-related topics to give their computing graduates competitive advantage with employers. Few exist currently, and none has achieved ascendant respect in the market. A meaningful credential must:
    - Align with the institution's aspirations.
    - Represent demonstrable skills.
    - Become a permanent part of the graduate's professional qualifications and transcript.
    - Require critical thinking and not merely "check the box" exposure to credentialing criteria.
    - Emphasize best practices and not mandated standards.
    - Support a mechanism for keeping knowledge and skills current and relevant.[4]

- A set of guidelines for degree programs in computer science, entitled CS2013, a collaboration between ACM and the Institute of Electrical and Electronics Engineers Computer Society (IEEE-CS) has taken an outward-facing approach to the development of the curriculum and has incorporated relevant cybersecurity concepts within the various computer science knowledge areas.[5]

Community Support

Development and adoption of a cybersecurity curriculum would be greatly aided by an organized community of practice combining industry, government, and academia. A committed and active community would help to coordinate initiatives, distribute tools, share courses and best practices, and provide funding and other resources.

Building an improved pipeline for a cybersecurity workforce will require a commitment from business and government to collaborate with educational institutions to provide:

- Funding
- Curriculum advice
- Courseware and software tools
- Internship and capstone experiences
- Mentoring
- Job opportunities

Table of Contents

Background

The reliable, secure exchange of digital information is vital to most human activity from banking to medicine to infrastructure management to elections. As the use of information technology expands, so also do the potential consequences of cyber attacks, and so does the need for a skilled workforce to prevent and defend against them. Unfortunately, the pool of available talent to build and certify applications designed to withstand attacks, diagnose and prevent security intrusions, and defend against cyber attacks, is inadequate to meet current needs. The pipeline is long and the flow is inadequate. Government agencies are scrambling to find sufficient qualified candidates for cybersecurity posts, especially in national defense and homeland security, and the private sector is similarly struggling to fill positions. Among the challenges:

- Despite the ubiquity of computers and the importance of cybersecurity to society, relatively few students pursue a BS or advanced degree in computer science or computer engineering, and fewer still choose to become expert in cybersecurity. Recent increases in computing students are an encouraging trend, but there is still need for growth.

- Many holders of master's and doctoral degrees in computer science and computer engineering (48.1% to 72.6% depending on degree and field of study) are nonresident aliens, unlikely to be granted security clearances required for many sensitive cybersecurity jobs in the United States.[6]

- Few PhD recipients in information assurance (IA) or cybersecurity return to academia to enrich the cybersecurity ecosystem, and fewer still join the teaching faculty to help educate future generations of cybersecurity experts.[7]

Both government and private industry are taking steps to identify, recruit, educate, and train cybersecurity professionals for the varied roles needed in the cybersecurity workforce. Here are some highlights of cybersecurity initiatives undertaken during the last few decades:

- In 1998, the NSA teamed with cybersecurity experts from academia and industry to create Centers of Academic Excellence in Information Assurance Education (CAE/IAE), later joining forces with the DHS to run this program. Accomplishing its mission to "reduce vulnerability in our national information infrastructure by promoting higher education and research in IA and producing a growing number of professionals with IA expertise in various disciplines"[8] has required broadening its curriculum standards beyond its original primary goal of setting and encouraging compliance with training requirements.

- NSF's CyberCorps® and its Scholarship for Service (SFS) program[1] that gives scholarships to promising computer science students with the requirement that they will work in government jobs for at least a specified time after graduation. Other cybersecurity education funding opportunities at the NSF include:
  - Advanced Technological Education (ATE) supports education in technical skills, including cybersecurity, mostly at technical colleges and other two-year institutions.
  - Secure and Trustworthy Cyberspace (SaTC) is a new cross-agency program that funds cybersecurity research and education.

Many worthy projects compete for these funds. How can NSF better use its resources to help remedy the cybersecurity pipeline problem? How can we enlist stakeholders—business, government, educational institutions—in the effort? What should cybersecurity education look like? What's the most productive balance between promoting awareness of cybersecurity issues

[1] NSF requires that a recipient of SFS can show equivalence to a CAE.

across a broad range of disciplines and educating cybersecurity experts? What knowledge areas need to be part of various curricula, and how should they be distributed among associate, bachelor, and postgraduate degree programs?

At the request of the NSF and through the coordination of the ACM, a group of cybersecurity experts gathered 21-22 February, 2013, in Atlanta, Georgia, to consider these and other questions, and to make recommendations for refocusing and reorganizing cybersecurity topics toward developing cybersecurity curricular guidelines for colleges and universities.

Previous Work Toward Cybersecurity Curriculum Guidance

Principles

The U.S. National Initiative for Cybersecurity Education (NICE) strategic plan puts forward objectives for "Building a Digital Nation" based on "…a trusted and resilient information and communications infrastructure."[9] One key objective (2.2) is to "…promote interest in computer science and cybersecurity by increasing diversity and quantity of course offerings and research opportunities."[10] The plan suggests five strategies to achieve this objective:

1. Increase the quantity and diversity of computer science courses in high schools
2. Increase the quantity and diversity of undergraduate and graduate cybersecurity curricula
3. Champion cybersecurity competitions
4. Advance excellence in cybersecurity research and development
5. Coordinate a learning network of virtual national cybersecurity laboratories

USACM, ACM's policy arm, emphasizes that educating students in the fundamentals and principles of cybersecurity and providing labs and experiences that encourage creative thinking are essential for building a diverse cybersecurity workforce. USACM opines that "Training in narrow techniques for specific networks and/or systems has its place in cybersecurity education, but it is only one facet of such education. It is not sufficient to focus on the symptoms of cybersecurity problems. A broad education that includes systems analysis and design is critical to prepare cybersecurity professionals for designing, implementing, and protecting the systems we rely upon."[11]

At an NSF-sponsored workshop in October 2010[12], cybersecurity stakeholders discussed additional principles for developing a cybersecurity workforce:

- Cybersecurity is an international issue.
- A multi-disciplinary approach is needed to integrate relevant cybersecurity issues into diverse disciplines such as forensic sciences, public policy, and law.
- Approaches are needed to address causes rather than symptoms of the continuing security breaches in computer systems.
- Better strategies are needed to integrate cybersecurity education and awareness throughout a lifetime of learning.

A cybersecurity curriculum will confront barriers:

- The university model does not completely satisfy all cybersecurity education and training needs. It often does not serve the needs of people who cannot leave the workforce to pursue a degree, nor does it accommodate short, intensive courses that respond to specific and current concerns.
- Academic departments are notoriously self-contained and reluctant to share resources, impeding collaboration and integration.

- Employers want cybersecurity graduates with real-world experience but are reluctant to provide that experience through internships or part-time work.
- International collaboration on cybersecurity issues is often hindered by national security concerns and legal issues such as conflicting laws governing patents and intellectual property.

Participants at the 2010 workshop offered suggestions for codifying the body of cybersecurity knowledge and identifying desirable learning outcomes.

A Summit on Secure Software held in Washington DC in October 2010[13] made a number of recommendations regarding a cybersecurity curriculum:

1. Increase the number of faculty who understand the importance of secure programming principles, and will require students to practice them.
2. Provide faculty support for the inclusion of security content through clinics, labs, and other curricular resources.
3. Establish professional development opportunities for college faculty, non-computer science professionals, and K-12 educators to heighten their awareness and understanding of secure programming principles.
4. Integrate computer security content into existing technical and non-technical (e.g. English) courses to reach students across disciplines.
5. Require at least one computer security course for all college students
    a. For computer engineering and computer science students, focus on technical topics such as how to apply principles of secure design to a variety of applications.
    b. For non-technical students focus on raising awareness of basic ideas in computer security.
6. Encourage partnerships and collaborative curriculum development that leverages industry and government needs, resources, and tools.
7. Promote collaborative problem solving and solution sharing across organizational (e.g. corporate) boundaries.
8. Use innovative teaching methods to strengthen the foundation of computer security knowledge across a variety of student constituencies.
9. Develop metrics to assess progress toward meeting the educational goals specified in the curriculum.
10. Highlight the role that computer security professionals should play in key business decision-making processes.

Topics and Risk Areas

Many universities and organizations shape their educational objectives in terms of knowledge areas in information assurance and cybersecurity. A few examples below illustrate the healthy diversity that currently exists.

At Carnegie Mellon University, the KSAs that guide curriculum development for its master's degree programs are organized into the following topics:[14] [15]

Assurance process and management

- Assurance across the life cycle
- Risk management
- Assurance assessment
- Assurance management

Assurance product and technology

- System security assurance
  - Potential attack methods
  - Analysis of threats to software
  - Methods of defense
- System functionality assurance
- System operational assurance

CMU offers a bachelor degree with a specialization in Software Assurance. It defines the degree as the "Application of technologies and processes to achieve a required level of confidence that software systems and services function in the intended manner, are free from accidental or intentional vulnerabilities, provide security capabilities appropriate to the threat environment, and recover from intrusions and failures [Mead 2010]."[16] The CMU curriculum's focus on software assurance is not an exemplar all schools will choose to follow, since it does not include education related to creating secure networks and protocols, forensics, non-technical security topics, or other non-software issues.

In February 2013, the UK Sector Skills Council, a trade organization for computing in support of business, recently put forth, via its National Skills Academy for IT, its own list of knowledge areas that must be included in the discipline of information security:

- Information governance
- Risk assessment and management
- Security development and Information security architecture
- Information security testing and information assurance methodologies
- Secure operations management
- Service delivery and vulnerability assessment
- Incident management, investigation, and digital forensics
- Information security audit

According to The Chartered Institute for IT (British Computer Society, BCS), this list is incomplete and lacking in organization. BCS noted that the list lacks an overall structure and omits information security management, business recovery, and security research.

Another UK institution beginning to formulate a curriculum for cybersecurity education is the Institution of Engineering and Technology (IET). The IET seeks to develop awareness of cybersecurity issues and practical skills in practicing engineers. Toward that end, the IET, with support from other professional computing associations, is investigating the feasibility of sponsoring young professional engineers and technologists to expand their professional skills and credentials by taking accredited postgraduate cybersecurity courses.[17]

One way of moving toward a cybersecurity curriculum is to look at the security challenges and risks that currently characterize cyberspace. The 2011 CWE/SANS Top 25 Most Dangerous Software Errors is a list of the most widespread and critical errors that can lead to serious vulnerabilities in software. The list is a product of collaboration among the SANS Institute, the MITRE Corporation, and other security experts.[18]

Insecure Interaction Among Components

Rank	Name
1	Improper neutralization of special elements used in an SQL command (SQL injection)
2	Improper neutralization of special elements used in an OS command (OS command injection)
4	Improper neutralization of input during web page generation (cross-site scripting)
9	Unrestricted upload of file with dangerous type
12	Cross-site request forgery (CSRF)
22	URL redirection to untrusted site (open redirect)

Risky Resource Management

Rank	Name
3	Buffer copy without checking size of input (classic buffer overflow)
13	Improper limitation of a pathname to a restricted directory (path traversal)
14	Download of code without integrity check
16	Inclusion of functionality from untrusted control sphere
18	Use of potentially dangerous function
20	Incorrect calculation of buffer size
23	Uncontrolled format string
24	Integer overflow or wraparound

Porous Defenses

Rank	Name
5	Missing authentication for critical function
6	Missing authorization
7	Use of hard-coded credentials
8	Missing encryption of sensitive data
10	Reliance of untrusted inputs in a security decision
11	Execution with unnecessary privileges
15	Incorrect authorization
17	Incorrect permission assignment for critical resource
19	Use of a broken or risky cryptographic algorithm
21	Improper restriction of excessive authentication attempts
25	Use of a one-way hash without a salt

In a similar vein, the Open Web Application Security Project, (OWASP) ranks web-based security risks that require the intervention of skilled practitioners. OWASP publishes guides for developers, testing, and code review that describe common web-based vulnerabilities. The OWASP consortium identified the ten most common web-related cybersecurity risk areas for 2013:[19]

Rank	Name
1	Injection
2	Broken authentication and session management
3	Cross-site scripting
4	Insecure direct object references
5	Security misconfiguration
6	Sensitive data exposure
7	Missing function-level access control
8	Cross-site request forgery (CSRF)
9	Using components with known vulnerabilities
10	Unvalidated redirects and forwards

An enumeration of vulnerabilities and risks will vary depending upon who is making the list. The usefulness of such lists for cybersecurity education is to inform discussions that address how to construct systems without vulnerabilities for threat agents to exploit. Solutions run the gamut from better design of networks and software to better documentation and user interfaces for system administrators.

Current Initiatives in Cybersecurity Education

A report of an Innovation in Technology in Computer Science Education (ITiCSE) workshop published in 2010[20] identified knowledge areas and associated subjects that would comprise the curriculum for information assurance. Information assurance is a broad category that encompasses cybersecurity and computer security. These terms are defined as follows:

Information Assurance	A set of technical and managerial controls designed to ensure the confidentiality, possession of control, integrity, authenticity, availability, and utility of information and information systems.[21]
Cybersecurity	The ability to protect or defend the use of cyberspace from cyber attacks.[22]
Computer Security	Measures and controls that ensure confidentiality, integrity, and availability of information system assets including hardware, software, firmware, and information being processed, stored, and communicated.[23]

In pursuing its goal of curriculum guidance for Information Assurance, the ITiCSE workgroup identified eleven knowledge areas:

- Fundamental concepts
- Cryptography
- Security ethics
- Security policy
- Digital forensics
- Access control
- Security architecture and systems
- Network security
- Risk management
- Attack/defense
- Secure software design and engineering

The ITiCSE working group refined these into 83 associated subjects.

A 2011 ITiCSE report[24] examined information assurance education in two-year and four-year colleges and universities. The working group used an institution's designation as a CAE (CAE-R

and CAE/IAE in the case of four-year institutions and CAE2Y in the case of community colleges) as evidence of the coverage of that institution's IA program.[25]

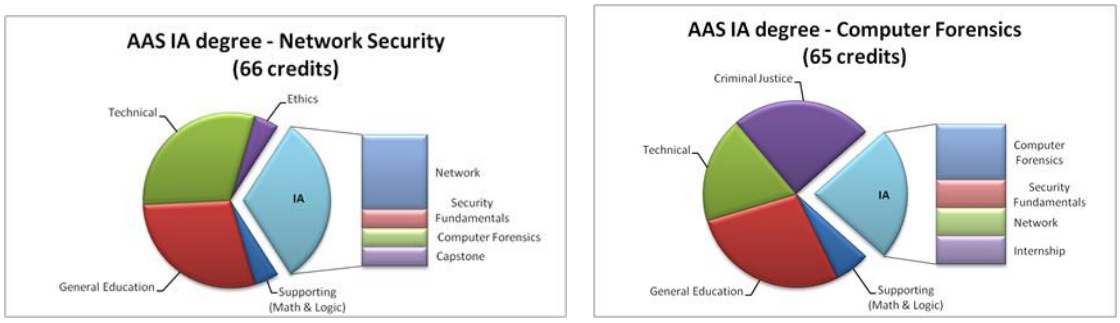
While this and other classification schemes help to facilitate discussion about cybersecurity curricula, no particular curriculum design has yet gained universal acceptance.

Observations on four-year programs
The working group identified 73 CAE institutions that offered programs with an IA track. Of these, 42 were offered by computer science departments, 16 by departments of computer information systems, five from security departments, and one each from schools or departments of informatics, software engineering, electrical engineering and computer science (EECS), and criminal justice. The titles of the degree programs varied widely.

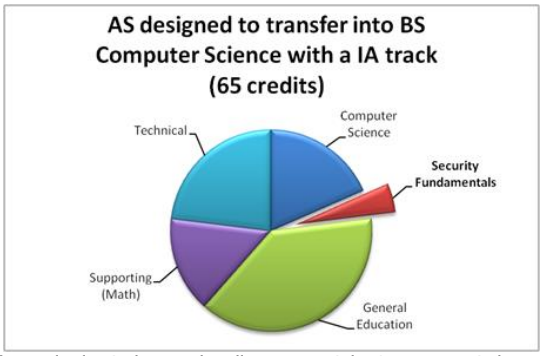
Although many computer science degrees included courses in security, there was no consistent curriculum for a baccalaureate degree in information assurance. The working group examined in detail seven baccalaureate degree programs with an information assurance track and found that they followed a typical computer science curriculum with security-related electives.

Typical IA programs included courses on security fundamentals and ethics. The security tracks varied between two and six courses, including electives that tended to be in the areas of network security, secure coding, cryptography, or privacy.

Observations on two-year programs
The working group compared the computer science course offerings at 16 community colleges, 14 of which graduated students with associate in applied science (AAS) degrees directly into jobs and two of which granted associate of science (AS) degrees to students intending to continue to bachelor degrees. These two curricula allocated their credit hours quite differently:



Comparison of credit hour requirements for typical AAS IA degrees in Network Security and Computer Forensics
ITiCSE-WGR'11, June 27-29, 2011, Darmstadt, Germany



Course content of a typical AS degree leading to a BS in Computer Science with an IA track
ITiCSE-WGR'11, June 27-29, 2011, Darmstadt, Germany

The typical associate degree program included a general course on computing, a course on security fundamentals and a networking course. Approximately half of all programs included courses on digital forensics, programming, general operating systems, and databases. Several institutions offered courses in ethical hacking, wireless security, and secure e-commerce.

Pilot cybersecurity articulation agreements such as a recent arrangement between Union County College and Stevens Institute of Technology, both in New Jersey, are showing promise. As with many fields of study, articulation agreements that permit seamless transfer of a student from a two-year program to a four-year baccalaureate program can be complicated. Widely accepted cybersecurity curricular standards or guidelines would facilitate this kind of institutional collaboration that benefits the colleges and universities, the transfer students, and the workforce pipeline.

Going beyond two-year degrees, most of the IA-related degrees seem to be at the graduate level, and particularly at the master's level.[26]

Workshop Objectives and Approach

The objective of the Atlanta workshop was to bring together a Core Leadership Group of cybersecurity experts to recommend actions that could improve the cybersecurity workforce pipeline. Workshop participants discussed the knowledge, skills, and abilities (KSAs) that a post-secondary school graduate should possess to enter the workplace as security-savvy technicians, IT managers, software developers, thought leaders, educators, or cyber defenders or warriors. (The workshop agenda appears in Appendix 1. A list of the Core Leadership Group and workshop organizers appears in Appendix 2).

The participants approached the workshop as an opportunity to brainstorm and to speak candidly of lessons learned about things that worked and things that did not work in their own experiences. The ideas that resulted are informal recommendations and do not necessarily reflect consensus among all who took part in the discussions. Indeed, some topics provoked spirited debate that resulted in varying or conflicting opinions. This report summarizes the opinions and recommendations discussed by the Core Leadership Group during the plenary discussions and feedback received from them on a preliminary draft of the report.

Report on Discussions

The workshop participants broke out into small workgroups to consider questions meant to provoke discussion, reveal points of contention, and encourage them to delve deeply into the salient issues. A plenary session followed in which each workgroup presented its opinions and recommendations for discussion by all workshop participants.

What are the cybersecurity-related sub-disciplines? What particular orientation would be associated with input from major disciplines such as computer science programs?

The workshop participants favored the term "knowledge areas" rather than '"specialty areas" or "sub-specialties," noting that the goal should be to unite rather than fragment a vital body of knowledge. In terms of organizing knowledge areas into a curriculum, workshop participants disagreed on whether the U.S. National Initiative for Cybersecurity Education (NICE) framework was a good starting point for organizing a cybersecurity curriculum.

NICE's National Cybersecurity Workforce Framework is a detailed and systematic categorization of cybersecurity knowledge areas. The NICE framework also defines a vocabulary and establishes a taxonomy for cybersecurity.[27] The seven categories of the framework group together related specialty areas—31 of them—each of which is further divided into dozens of KSAs. It cross-references these specialty areas and tasks to occupational responsibilities and job titles.

For some Atlanta workshop participants, the NICE framework is a useful categorization of topics and related skills, and a good starting point from which to build a cybersecurity curriculum. Others cautioned that a simpler categorization scheme would better guide curriculum development. These should appear in an introductory general security course, followed by courses focused on evolving communities of practice:

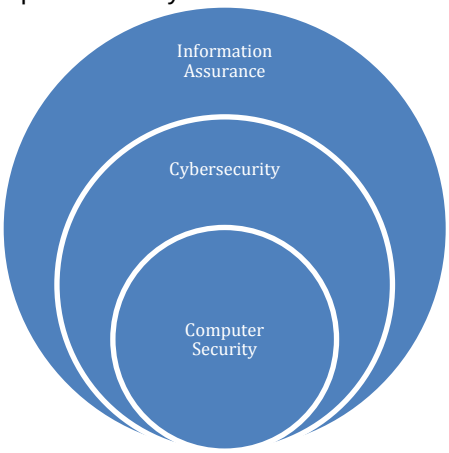
- Digital forensics
- Penetration testing
- E-evidence
- Perimeter defense
- Secure coding and software security
- Management of security

One workshop participant warned that if the list of knowledge areas goes too far beyond this short laundry list, there is a risk of diluting the content.

In the general discussion, participants voiced the need for a holistic perspective on cybersecurity, and for further research and education on building systems that are resistant to cascading failures.

Participants in one of the workshop's working groups contributed a classification scheme they felt struck the right balance of granularity and structure. This categorization scheme uses the same category definitions as the 2010 ITiCSE workshop described earlier in this report,[28] and expands on the previous workshop's knowledge areas.

The classification scheme can be visualized as nested sets of knowledge areas, with information assurance wholly encompassing the field of cybersecurity, which in turn fully contains all knowledge areas in computer security.



The table below shows the primary categorization of each knowledge area. Many knowledge areas have aspects that make them applicable to multiple categories. For example, if a database is part of the system, it is part of the foundational architecture. Many aspects of wireless security are built into the hardware platform. There are many other examples of how knowledge areas overlap multiple categories. Institutions using this or a similar list of knowledge areas are likely to

re-categorize them based on their specific departmental structure and learning objectives.

	Categories		
Knowledge Areas	Computer Security	Cybersecurity	Information Assurance
Operating systems	x		
Embedded systems	x		
Networks & network security	x	x	
Databases	x	x	
Programming	x		
Data mining / big data / analytics		x	
Forensics		x	
Cryptography	x	x	
Ethics			x
Policy	x		x
Access control	x		
Security architecture	x	x	x
Risk management		x	
Threats / attacks / defenses	x	x	
Operational issues	x		x
Legal framework		x	x
Data governance			x
Secure software design and engineering	x	x	x
Economics			x
Malware Intrusion Detection Systems Intrusion Protection Systems		x	
Botnets		x	
Web			x
Wireless	x		x
Mobile / cloud		x	
Sociology			x
Applications ○ Healthcare ○ Finance ○ Critical infrastructures		x	
Cyber warfare	x	x	

The Core Leadership Group made some observations related to choosing and organizing cybersecurity knowledge areas:

- Programs in computer science, software engineering, information systems, and other areas could contribute to cybersecurity education by offering one or more modules covering aspects of cybersecurity knowledge areas.
- Reverse engineering can play an important role in investigating security breaches.
- Analyzing network traffic is an important skill.
- The community of cybersecurity professionals should consider the limits of what is possible in achieving security.
- The ethical issues associated with cybersecurity are deep and complicated.
- Knowledge of how to achieve reliable security is incomplete to say the least, and technical issues abound, such as where to position an audit function (operating system, database, etc.), when it should be turned on, what it should record, how does an operating system protect itself from attack, and many more.
- Assessing risk and risk management are different, complicated tasks.
- Training in cyber defense as well as attacks (blue vs. green) and cyber warfare gaming offer important opportunities to develop and refine appropriate skills.

What fundamental "ways of thinking" should institutions engender by effective education in cybersecurity? What are the implications of the importance of these topics for education?

To protect systems and build penetration-resistant applications, we need to temporarily adopt the thinking process of the malevolent hacker. "How can I get inside this network? How can I make the system fail?" This is the mission of the penetration tester; discovering vulnerabilities in a software product or a computer system to learn how to defend against a cyber-attack that exploits them. Several members of the Core Leadership Group opined that diverse thinking and backgrounds—not merely an adversarial attitude--are needed in cybersecurity. A Google product security manager related her company's extensive use of the hack-to-defend approach, and the difficulty in recruiting the right kind of people to excel at this unconventional occupation. The people who possess the ability to seek and remedy cyber-vulnerabilities are usually characterized by a passion for figuring out how things work. They can sometimes appear to be underachievers—but not always. The dichotomy of cracker/hacker that discounts academic achievement as anathema to adversarial, "out-of-the box" thinking is a stereotype that may well be limiting the diversity of students pursuing careers in cybersecurity[29]. These nonconformist students might profit from alternative, more hands-on learning styles outside the traditional lecture/lab model.

Attack/defense cyber-game competitions are sometimes able to inspire interest in the adversarial aspects of cybersecurity, but this combative approach can turn off those who prefer collaboration to aggression. Moreover, this cat-and-mouse approach fosters an attitude of "penetrate and patch" rather than an understanding and appreciation for principles-based constructive security. There is another kind of adversary, able to think carefully, lay long-range plans, and leverage social situations to their advantage. This suggests a different type of contest, where the goal is to build something that meets specific requirements. The team would comprise constructers and testers, the testers being the "penetration testers" collaborating with the constructers to find and remedy vulnerabilities. The team would be evaluated as a whole, thus eliminating the benefits of the penetration testers trying to "win" against the constructors; everyone would have to see others as colleagues rather than adversaries.

Other important matters that deserve serious thought include:

- Recognizing that we do not know how to build truly secure and resilient computer systems and that we realize limits exist to what tools and practices can accomplish;
- Recognizing that assessing the risk of cyber threats can be very different from assessing risk in traditional engineering contexts;
- Recognizing the risks of using usual tools outside their intended usage or of using unusual tools such as unfamiliar compilers;
- Recognizing a particular set of security issues in a distributed and/or parallel environment;
- Security within the sphere of human-computer interactions;
- Insider threats and the roles of psychology, sociology, and psychiatry in preventing or combating them;
- Complacency: the assumption that lack of apparent security problems does not equate to lack of risk.

To what extent can a technical computer science curriculum, if "tightened up," address the issues of cybersecurity? If so, how? What are the recommendations of the Leadership Group in this regard?

At the Atlanta workshop, participants received an update on the development of CS2013, the latest curriculum guidance on computer science produced for institutions of higher education by the ACM Education Board and the IEEE Computer Society. The publication schedule for the final version of the document is the fourth quarter of 2013. Several of the report's authors presented the current state of the project based on the Ironman version of the report.[30]

The CS2013 authors developed a new knowledge area titled "information assurance and security" (IAS), and within it have organized topics vital to cybersecurity. In CS2013, IAS education includes "…all efforts to prepare a workforce with the needed knowledge, skills and abilities to protect our information systems…"[31] Of necessity, they have had to place limits on the time recommended for study of each subject, but a wide range of subject choices is available to institutions adopting CS2013. Indeed, different computer science or computer engineering departments will have different curricula, and it will be up to each department to decide what topics it wants to emphasize and how to do it.

CS2013 distributes cybersecurity topics throughout the curriculum. The knowledge areas for a computer science curriculum are:

AL	Algorithms and Complexity	AR	Architecture and Organization
CN	Computational Science	DS	Discrete Structures
GV	Graphics and Visual Computing	HC	Human-Computer Interaction
IAS	Information Assurance and Security	IM	Information Management
IS	Intelligent Systems	NC	Networking and Communications
OS	Operating Systems	PBD	Platform-based Development
PD	Parallel and Distributed Computing	PL	Programming Languages
SDF	Software Development Fundamentals	SE	Software Engineering
SF	Systems Fundamentals	SP	Social and Professional Issues

The knowledge areas are further subdivided into knowledge units, which are then refined into topics, and then into learning outcomes, the most specific and detailed level of refinement.

CS2013 refers to mandatory courses that every computer science student must study as "core" courses, each accorded one or more core hours. There are two types of core hours:

- **Core Tier 1 hours** should be included in all computer science programs of study.
- 80% of **core Tier 2 hours** should be included in a computer science program of study, and institutions may pick and choose from a list of topics:

IAS topics	Core Tier 1 hours	Core Tier 2 hours	Associated electives?
Foundational concepts in security	1		
Principles of secure design	1	1	
Defensive programming	1	1	yes
Threats and attacks		1	
Network security		2	yes
Cryptography		1	
Web security			yes
Platform security			yes
Security policy and governance			yes
Digital forensics			yes
Secure software engineering			yes

The CS2013 developers associated electives with many of the topics—those with a "yes" in the rightmost column. They also embedded many cybersecurity topics in other key knowledge areas such as:

- Software development fundamentals
- Software engineering
- Programming languages
- System fundamentals
- Parallel and distributed computing
- Networks and communications
- Operating systems

In this security-across-the- curriculum approach, a degree in computer science would require 26 core Tier 1 hours and 52 Tier 2 hours devoted to topics in information assurance and security.

The current version of the CS2013 document, called Ironman 1.0, has nearly seventy examples of field-tested courses that cover various parts of the body of knowledge. The final version will also include some curricular exemplars that will illustrate how a whole set of classes at an institution maps to the body of knowledge. Since different institutions have different needs and often organize their curricula in different ways, the authors wanted to offer practical guidance rather than a stylized, untested course model. CS2013 uses exemplars; pointers to actual classes taught successfully, with their covered topics mapped to the IAS body of knowledge. To support uptake of its recommendations, the CS2013 team continues to gather exemplars of courses and curricula representing best practices in particular topics, and to assemble materials to assist, guide, and support course offerings. The CS2013 report may also be a guide to cybersecurity topics that might form the basis for minors or credentials.

The Atlanta workshop participants felt that the approach to cybersecurity education developed in CS2013 was highly desirable and that it provides a sound basis for more advanced study of cybersecurity subjects and some guidance for such study. Material from the CS2013 report is likely to find its way into future curriculum recommendations from the ACM, the IEEE Computer Society, and the Association for Information Systems on software engineering, computer engineering, information systems, and information technology. Workshop participants offered some suggestions for the ongoing evolution of CS2013. They felt that:

- Every undergraduate—in any degree program—should be aware of the basic principles of cybersecurity and the vulnerabilities of cyberspace. They should receive a non-technical course addressing these issues.
- Every computing student should receive at least one technical course on aspects of cybersecurity.
- Many textbooks on AI, networks, databases, operating systems, and other areas of computer science, have chapters on “security.” These chapters need to receive adequate treatment in the associated course.
- Although an integrated, disciplined approach to cybersecurity and a systems perspective as developed in CS2013 are very important, there is a danger that by embedding cybersecurity topics within other computing courses, security as a separate topic could “disappear” or receive inadequate attention, if a dedicated course is not also included.
- It will be important to characterize the eventual formal curriculum recommendations as guidance and not as mandatory elements of a certification or regulatory scheme.

What topics would *not* typically appear in the manner outlined in the previous question? Which of these topics are fundamental to education in cybersecurity?

Recognizing and handling common vulnerabilities, digital forensics, incident management, security fundamentals, the legal and ethical issues associated with cybersecurity, audit, and economics issues are all topics that would not ordinarily be part of a computer science or information systems curriculum.

Most of the cybersecurity knowledge areas and "ways of thinking" described earlier in this report could be covered in some combination of computing courses. It may prove difficult to cover a wide range of the material to the desired depth. Much will depend on the orientation of a particular department and a particular program. For instance, there needs to be education for aspiring computing professionals and for those who have a concern for the societal implications of cybersecurity. However, recognizing common vulnerabilities and knowing how to respond to them are fundamental knowledge all undergraduates should possess. Workshop participants suggested:

- It would be useful to have programs that address a subset of cybersecurity concerns; digital forensics or network security, for instance; such programs would require specialized core material.
- There is also a place for IT-related cyber operations programs with a practical orientation that emphasizes using systems rather than designing or building them.
- In the days before each student brought a laptop and a smartphone to school, courses such as "computers and society" promoted cyber literacy. Today, a course in "computers and security" would be a good way to promote awareness of cybersecurity issues throughout society. These courses could be tailored to address issues relevant to other disciplines; cybersecurity in medicine, in law, and others.

Can these topics (identified in the previous question) form the basis of a program minor to accompany a major in computer engineering / computer science / information systems / software engineering / information technology?

The Core Leadership Group took the view that it is important to heighten the profile of cybersecurity and to encourage students to courses and careers relevant to that field. At the same time, students who will become cybersecurity experts need to possess a sound basic education in their chosen computing discipline (computer science or software engineering, for example). Within these disciplines there should be fundamental core courses in cybersecurity and also options to focus specifically on security-related topics such as the IAS topics recommended by CS2013.

Credentials signifying mastery of particular knowledge areas within cybersecurity might serve to give certified graduates a competitive advantage in finding jobs. No credential has yet taken a fully dominant position in the market, though some are more widely adopted than others. Another challenge with credentialing is that today's best practices all-too-quickly evolve into tomorrow's anachronisms. A credentialing organization representing a community of practice needs to vet graduates for mastery and credentials for relevance to sought-after expertise. A recent article described characteristics for a successful credentialing process.[32]

- "Obtaining a credential requires years of post-bachelors education, in which the curriculum has been set by the most respected thinkers and practitioners in the field.
- "Credential holders are required to stay current with the latest developments in the field by continuing their education through courses sanctioned by the institution that issues credentials.
- "The threat of legal action to individuals (including malpractice litigation) incentivizes professionals to engage in best practices."

A credential is most useful if it appears on the student's transcript so the institution's reputation—and that of the credentialing organization, if different—adds force to the credential. Credentials also carry more weight when relevant to the skills employers are looking for. For this reason, it is important for educational institutions to maintain connections with employers; it is also important to have insights into workplace needs.

Would guidance on the above suffice to address the issues of cybersecurity education? If not, why not? How can uptake be encouraged?

Among U.S. institutions, the breadth of undergraduate subjects required for a computing degree leaves less than 40% of classroom time for computing topics. The situation is similar internationally. Yet high-quality cybersecurity education requires expertise across a considerable range of topics, is rigorous and demanding, and is labor-intensive for both students and faculty. There is too little time available in undergraduate programs to address the totality of expertise required for a meaningful concentration in cybersecurity.

Offering credentials is one way to stimulate uptake of a cybersecurity curriculum. In departments with a high profile in security-related activity, there is likely to be a visible and effective effort to recruit students to cybersecurity. In departments without a strong security profile, the Core Leadership Group recommended appointing an ambassador or advocate for cybersecurity. This person's task would be to encourage the study of and attention to security-related matters. For example, the advocate would encourage the inclusion of cybersecurity topics in the curriculum, uptake of security-related projects, and cybersecurity seminars. The advocate would operate a clearinghouse for information about internships, competitions, and job opportunities. The position of cybersecurity advocate is an opportunity for a young faculty member to make an important contribution to the department's reputation and its ability to compete for students.

Does the Core Leadership Group recommend the development of curricular guidance for baccalaureate and / or associate degrees in cybersecurity? Does the Group have any recommendations / guidance about what form this may take? How might ACM and other organizations encourage and facilitate the development of such courses? What would be the characteristics of high-quality programs in the area? How can faculty members develop expertise in this area be developed?

The Core Leadership Group agreed that an undergraduate curriculum is not conducive to a major in cybersecurity. Cybersecurity studies at the undergraduate level does not provide enough substance to merit a degree in itself, and a four-year Computer Science degree is too loaded to accommodate more than a general awareness of cybersecurity issues. That being the case, the Atlanta workshop participants discussed whether offering an optional fifth year with the last year focused on cybersecurity would benefit the schools, their students, and/or the job market. The consensus was that this idea would probably not work, because it would be hard to demonstrate that the cost and additional time spent in school required for this extra year would pay off for the students by providing more job opportunities, a higher salary, or a faster career path.

At the associate degree level, two-year colleges are as doing an excellent job of training cybersecurity technicians. Nearly thirty community colleges have earned the CAE2Y designation, and that number is growing. Other cybersecurity efforts by two-year colleges include CyberWatch and the Center for Systems Security and Information Assurance (CSSIA) within the NSF-funded Advanced Technological Education (ATE) centers. These programs join industry, government, and educational institutions for the purpose of increasing the quantity and quality of a workforce skilled in information assurance and computer forensics. There was consensus that two-year colleges are accomplishing a vital mission that deserves encouragement and support from business and government.

Technical certificates would help graduates market their skills to prospective employers. In the final analysis, the marketplace will judge the quality of an institution's cybersecurity training, and the value of an institution's brand will rise or fall based on its reputation for producing well-trained

graduates. The majority of the Core Leadership Group did not see the need for new curricular guidelines for cybersecurity at this stage in its evolution because:

- CS2013 already contains curricular guidance for aspects of cybersecurity.
- The subject is intellectually immature and still evolving.

A dissenting participant expressed the view that creating associate degree curricular guidance in cybersecurity beyond CS2013, particularly from the IT side, would be of tremendous benefit.

The group agreed that currently the field of cybersecurity lacks a cohesive community of interest. The Atlanta workshop participants suggested that professional societies have a very important role in fostering and supporting the development of communities of cybersecurity professionals. Forming a community is a necessary precursor to developing a cybersecurity curriculum. A community of practice will help determine best practices and devise effective strategies for teaching them. It will provide access to tools, resources, and continuing professional development, an activity that could help faculty members improve their cybersecurity expertise. A common basis in theory for these practices will enable the state of the art to evolve, and eventually anticipate, changes in technology and society that impact practice.

Several cybersecurity communities already exist, such as the Colloquium for Information Systems Security Education (CISSE), CyberCorps® programs hosted by the NSF, and the National Institute of Standards and Technology's (NIST), National Initiative on Cybersecurity Education (NICE) program. CISSE, a large organization with broad participation from private industry and government agencies, is a good place for government and industry to connect with college faculty.

Ensemble: An example of a community-building tool

At the Atlanta workshop, principal investigators of the Ensemble computing portal promoted Ensemble as a tool for building a community of practice among cybersecurity educators. The Ensemble project, headquartered at Villanova University, facilitates sharing of courses, resources, tools, knowledge, and ideas, and provides a forum where all cybersecurity constituencies can contribute for mutual benefit. Ensemble archives and cross-references courses, sample class materials, software tools, textbooks, reports, and other documents of interest to computing communities. Institutions can clone courses and contribute their work to the pool of available resources. It should be a responsibility of the cybersecurity community of practice to vet ideas and information available through resource-sharing tools such as Ensemble to ensure they are reliable, relevant, and meet quality standards.[33]

The CS2013 curriculum guidance documents currently reside on Ensemble for review and comments.[34]

Is there a place for encouraging the development of suitable master's-level courses and programs? If so, what should be their focus? Is the provision of curricular guidance here a priority?

The Core Leadership Group took the view that suitable master's courses were the main vehicle needed to produce graduates highly qualified in cybersecurity. One set of courses, building on a solid undergraduate background in computer science or related area, would educate a workforce of cybersecurity professionals with sophisticated skill sets. Courses could and should address:

- **Cybersecurity for computing professionals**…
  …emphasizing technical degree programs
- **Cybersecurity in society**…
  …emphasizing the threats within society, how to guard against them, and how to respond if necessary
- **Cybersecurity operations**…
  …focusing on deploying appropriate technology and offering advice on preventing security breaches rather than on cryptography, building resilient systems, and other deeply technical issues

These various programs prepare graduates to pursue cybersecurity job opportunities such as those posted on "cybersecurity careers."[35] A sampling of the web site's job categories includes:

- Cybersecurity consultant
- Network security
- Operations and security management
- Incident and threat manager
- Systems architect
- Risk analysts and risk manager
- Forensic analyst
- Education and training manager

In many of these roles, experts will use appropriate security analytics tools to postulate, detect, investigate, analyze, or remediate threats.

What advice can the Group offer in relation to workforce needs…

- **…in particular areas of cybersecurity?**
- **…at particular levels of education (associate degree, baccalaureate degree, master's degree, PhD)?**

Associate, bachelor, master's, and doctoral degrees all have their vital roles to play in educating a multifaceted cybersecurity workforce. In particular, doctoral degrees are critical to support next-generation education and research within academia, and to provide advanced expertise necessary for industry and government. Programs are needed at all levels, but there is a particular need for individuals with these skills:

- *Ability to think set and achieve long-term research goals*.
  The trend toward short-term funding horizons makes it critical for doctoral students to

learn how to establish visionary research programs given modern time limits on most available funding. This is particularly important in cybersecurity, where time horizons are extremely short yet the need for fundamental change is extremely high.

- *Ability to achieve technology transition between research stages*.
  In many areas there has been a divergence between the theoretical foundations of cybersecurity and the eventual application of it to challenging real-world needs. Not every researcher needs to move from basic idea to implementation, but there should be some notion of advancement outside a specific research community, both taking in ideas and disseminating them more broadly.
- *Ability to combine theoretical and practical understanding*.
  Too often theory and practice are separated from one another in the advanced academic environment, yet both are necessary. Doctoral programs that instill a solid capacity to identify hypotheses and follow them up with both theoretical analysis and field studies or experiments are needed, both to inform policy makers and to assess whether innovations and scientific advances provide the hoped-for improvements.
- *Willingness to think beyond academia for career aspirations, and a willingness to cross over into other disciplines*.
  Too often doctoral students feel they disappoint their advisors if they choose a career outside the ivory tower. However, there are research careers performing, leading, and applying research throughout industry and government at all levels, whether for national security purposes or to advance innovation; the challenges in these spaces are certainly worthy of the talents of our best and brightest.

Related to the above:

- **How can uptake of recommendations for education in cybersecurity be encouraged?**

The Core Leadership Group recognized that curricular guidelines have value only to the extent that they guide actual curriculum development. The cybersecurity community needs to encourage uptake of educational recommendations proactively, through scholarships, internships, competitions and challenges, and the granting of credentials.

- **Is there essentially a new discipline associated with cybersecurity?**

Cybersecurity is not yet a discipline. It is still an immature field lacking a cohesive intellectual body of activity and clear underlying science. Its techniques and approaches strongly resemble those of various branches of engineering. Cybersecurity knowledge areas fit well within existing computing departments.

Conclusions

During the Atlanta workshop, participants discussed cybersecurity as a discipline, as an area of academic study, and as a public good in need of a large, expert workforce. Group discussions of diverse opinions and perspectives produced general agreement on the following issues:

- The Core Leadership Group identified the main elements (*i.e.* knowledge areas or sub-disciplines) of cybersecurity and emphasized the important fact that it is a multidisciplinary subject.
- Cybersecurity is currently an immature and ill-defined subject and not a true discipline since it lacks some of the criteria normally applied to disciplines.
- The "mind set" of the cybersecurity professional is an important factor in preventing, detecting, and mitigating security breaches. Developing this way of thinking must be part of recruiting and educating cybersecurity professionals.
- Every citizen and institution has a role to play in cybersecurity; its comparison with public health is worth exploring. Everyone, and in particular all students, should have some form of cybersecurity education.
- There is need for a whole variety of academic degree programs in cybersecurity from the technical aspects through to courses based on psychology, psychiatry, criminal justice, business (*i.e.* policy and economics) and more.
- Technical courses are necessary for producing high-quality graduates who can develop as computing professionals into cybersecurity experts of the future, crucial for protecting vital assets. The scope of cybersecurity education must also include programs for the computing professional, for operations staff, and to provide for the public good and the needs of society.
- Deeply technical courses at the master's and doctoral levels are needed to produce high-quality cybersecurity graduates capable of addressing the most sophisticated technological cybersecurity issues.
- Two-year colleges serve a very important need in the cybersecurity education pipeline and deserve encouragement to continue their work.
- Institutions of higher education should put effort into drawing the attention of computing students to the challenges of cybersecurity. The Core Leadership Group felt that all computing graduates should have at least one technical course in cybersecurity.
- The attention to security within the various knowledge areas in the CS2013 curriculum is a positive development likely to influence curricular guidance in computing areas such as software engineering, computer engineering, and information technology.
- Credentials, properly vetted by a governing body and carrying the imprimatur of a respected institution, can attract students to cybersecurity and help advance their careers. These credentials need to be challenging for students and to be seen as addressing deep issues in the area.
- Cybersecurity education requires a lot of hands-on activities; experiential, guided learning that is time- and labor-intensive for both students and faculty. It will be expensive, so sources of public and private funding should be sought to help talented students afford their education to the level they desire. In order for students to get hands-on training, some mechanism needs to be found to fund and provide access to current commercial equipment and tools (hardware and software) and data at all levels of higher education.
- There is a continuing need for doctoral graduates in cybersecurity, and to encourage them to remain in academia to help educate the high-quality cybersecurity graduates of the future.
- Cyber competitions and awards have an important role to play in motivating students toward cybersecurity careers.
- Building a community of practice is a necessary early step in establishing cybersecurity as a profession and in designing curricula to teach it. Toward that end, stakeholders should leverage existing professional organizations and resource-sharing projects. One

valuable tool that should be considered is Ensemble, a web portal providing access to course materials (including those planned for CS2013), publications, reports, case studies, textbooks, course exemplars, and more.

Recommendations

The Core Leadership Group developed specific recommendations for stakeholders to explore toward educating an excellent cybersecurity workforce:

For Institutions of Higher Education

- Educational institutions should be encouraged to support master's and doctoral degree programs in fields requiring cybersecurity knowledge and skills. They should be encouraged to draw the attention of students to the importance of cybersecurity as a career and as an area of study by:
    - Embracing the security recommendations within the forthcoming CS2013 report
    - Offering respected credentials in the general area of cybersecurity
    - Where there is no particular research focus on security, putting in place a cybersecurity ambassador or champion whose role is to stimulate activity in and attention to security matters, both in the student body and in the curriculum
- Universities and professional schools should provide opportunities for faculty to take leaves to pursue projects that will bring benefit to the cybersecurity education community.

General

- In support of high-quality master's and doctoral programs, stakeholders including government and business should partner with educational institutions to provide internships, capstone experiences, adjunct faculty, funding, and access to resources.
- Government, industry, and other stakeholders should help students afford graduate degrees in cybersecurity.
- Since cybersecurity is still at a formative stage in its evolution, the Core Leadership Group (with one dissention) felt it premature to produce curriculum guidelines beyond CS2013.

For the National Science Foundation

- NSF should consider providing several (say, three) Massive Open Online Courses (MOOCs) that can assist in teaching fundamental material on cybersecurity. The precise nature of these should be informed by resources supplied by CS2013 exemplars.
- NSF should leverage the CyberCorps® Scholarship for Service (SFS) program so that graduates with advanced degrees—especially doctorates—can fulfill their service obligation in academia, contributing toward improving cybersecurity education and transferring their knowledge to a younger cohort of students.
- NSF should further encourage and support two-year colleges in their efforts to improve and broaden access to cybersecurity education.
- NSF should continue support for cybersecurity challenges and competitions.
- At a more general level, NSF should support research into better insights for building secure and resilient computer systems, including those that exploit distributed and/or parallel processing capabilities. Researchers involved in such projects would be required to share beneficial developments of their work with the cybersecurity education community.

Acknowledgements

Appendix 2 lists the workshop participants to whom the writers of this report are extremely grateful for their time and expertise. Yan Timanovsky coordinated the logistical arrangements for the workshop including travel and lodging and managed the writing of this report. Thanks also to members of the leadership group who helped plan the workshop but were unable to attend ("regrets" in the appendix). Grateful acknowledgement is made to John Impagliazzo, Matt Bishop, Melissa Dark, Deborah Frincke, Beth Hawthorne, Cynthia Irvine, Stephen Northcutt, and Chuck Pfleeger, who contributed comments and corrections to a preliminary draft of this report.

Appendix 1
Workshop Agenda

Thursday 21st February 2013

09:00 – 09:15	**Welcome and introductions**		
09:15 – 09:30	**Background to project**		Andrew McGettrick
09:30 – 10:00	**Initiatives affecting cybersecurity education**		Victor Piotrowski
10:00 – 10:30	**Discussion of the pre-meeting documentation** Are the questions appropriate? Additional questions?		
10:30 – 10:45	**BREAK**		
10:45 – 12:00	**Discussion of Questions 1, 2** Working Group 1	**Discussion of Questions 1, 2** Working Group 2	**Discussion of Questions 1, 2** Working Group 3
12:00 – 12:30	**PLENARY** Discussion of recommendations from working groups		
12:30 – 13:30	**LUNCH**		
13:30 – 14:00	**Industry perspective on cybersecurity**		Parisa Tabriz
14:00 – 15:15	**Discussion of Questions 3,4,5,6** Working Group 1	**Discussion of Questions 3,4,5,6** Working Group 2	**Discussion of Questions 3,4,5,6** Working Group 3
15:15 – 15:45	**PLENARY** Discussion of recommendations from working groups		
15:45 – 16:00	**BREAK**		
16:00 – 16:30	**Information Assurance and Security within CS2013**		Beth Hawthorne
	Cybersecurity Education in Community Colleges		Beth Hawthorne
16:30 – 17:00	**A few ideas about security in higher education**		Stephen Northcutt

Friday 22nd February 2013

09:00 - 09:30	**Demonstration of Ensemble**		Lillian "Boots" Cassel Lois Delcambre
09:30 – 10:45	**Discussion of Questions 7,8,9** Working Group 1	**Discussion of Questions 7,8,9** Working Group 2	**Discussion of Questions 7,8,9** Working Group 3
10:45 – 11:00	**BREAK**		
11:00 – 12:00	**PLENARY** Discussion of recommendations from working groups		
12:00 – 12:15	**Additional considerations** Are there any additional matters that merit consideration? Recommendations about future activity		
12:15 – 12:30	**Next steps**		
12:30 – 13:00	**LUNCH**		

Appendix 2
Workshop Participants / Core Leadership Group

MEETING COORDINATOR

Andrew McGettrick
Professor
University of Strathclyde
Chair, ACM Education Board
andrew.mcgettrick@strath.ac.uk

FOR THE NATIONAL SCIENCE FOUNDATION (NSF)

Victor Piotrowski
Education and Human Resources Directorate
vpiotrow@nsf.gov

Keith Marzullo
Division Director for Computer Network Systems
kmarzull@nsf.gov

Jane Prey (regrets)
NSF
janeprey@gmail.com

FOR THE ASSOCIATION FOR COMPUTING MACHINERY (ACM)

Lillian "Boots" Cassel
Professor, Computing Sciences
Villanova University
ACM Education Board
Ensemble Principal Investigator
bootscassel@gmail.com

Lois Delcambre
Ensemble Team Member
Portland State University
lmd@cs.pdx.edu

John Impagliazzo
Professor Emeritus
Department of Computer Science
Hofstra University
ACM Education Board
John.Impagliazzo@hofstra.edu

Mehran Sahami (participated by telephone)
Stanford University
sahami@cs.stanford.edu

Yan Timanovsky
ACM Education Manager
timanovsky@hq.acm.org

Cameron Wilson
ACM Director of Public Policy
wilson_c@hq.acm.org

CORE LEADERSHIP GROUP

Matt Bishop (regrets)
Professor, Department of Computer Science
University of California at Davis
Co-director of University's Computer Security Lab
bishop@cs.ucdavis.edu

Hsinchun Chen
Director of Artificial Intelligence
College of Management
University of Arizona
hchen@eller.arizona.edu

Melissa Dark
Associate Professor in Computer Technology
Assistant Dean in the School of Technology
Purdue University
dark@cspurdue.edu

Ron Dodge (participated by telephone)
Colonel, Academy Professor
West Point CIO and Associate Dean, IT
United States Military Academy
ronald.dodge@usma.edu

Deborah Frincke (regrets)
Deputy Director, Research Directorate
U.S. Department of Defense
dafrinc@nsa.gov

Elizabeth K. Hawthorne
Senior Professor of Computer Science
Union County College
Chair, ACM Committee for Computing Education in Community Colleges
ehawthorne@acm.org

Cynthia Irvine
Chair, Cyber Academic Group
Naval Postgraduate School
Irvine@nps.edu

Stephen Northcutt
Director of Academic Advising
SANS Institute
Stephen@sans.edu

Chuck Pfleeger
Pfleeger Consulting Group
Former Professor at University of Tennessee
chuck@pfleeger.com

Fred Schneider
Professor and Chief Scientist of TRUST scientific technology center
Cornell University
fbs@cs.cornell.edu

Eugene Spafford (regrets)
Professor
Purdue University
Chair, ACM's U.S. Public Policy Council
spaf@purdue.edu

Parisa Tabriz
Chrome Security Engineering Manager
Google
parisa@google.com

Ray Vaughn
Associate Vice-President for Research
Mississippi State University
vaughn@research.msstate.edu

Endnotes

[1] National Initiative for Cybersecurity Education (NICE) Strategic Plan: *Building a Digital Nation.* September, 2012. http://csrc.nist.gov/nice/documents/nicestratplan/nice-strategic-plan_sep2012.pdf

[2] Piotrowski, Victor. *Remarks on the US Cybersecurity Education Landscape*. [PowerPoint slides] Presented February 21, 2013

[3] Mulligan, D. Schneider, F. *Doctrine for Cybersecurity.* Daedalus. Fall 2011, 70-92
Also available as Cornell Computing and Information Science Technical Report, April 2011.
www.cs.cornell.edu/fbs/publications/publicCYbersecDaed.pdf

[4] Schneider, Fred B. *Labeling-in Security*. IEEE Security & Privacy 7(6): 3 (2009)

[5] *Computer Science Curricula 2013 (CS2013).* ACM/IEEE-CS Joint Task Force
http://www.cs2013.org

[6] Ibid. #2

[7] Ibid. #2

[8] See http://www.nsa.gov/ia/academic_outreach/nat_cae/index.shtml

[9] Ibid. #1

[10] Ibid. #1

[11] USACM. Letter to Congress on Cybersecurity Legislation
http://usacm.acm.org/images/documents/2012CybersecurityStatement.pdf

[12] Lance J. Hoffman, *Building the Cyber Security Workforce of the 21st Century: Report of a Workshop on Cyber Security Education and Workforce Development*, Report GW-CSPRI-2010-3, Cyber Security Policy and Research Institute, The George Washington University, December 2010

[13] Burley, D. Bishop, M. *Summit on Education in Secure Software Final Report*. (GW-CSPRI-2011-7) (CSE-2011-15) June 30, 2011.
http://nob.cs.ucdavis.edu/bishop/notes/2011-sess/2011-sess.pdf

[14] Mead, Nancy, Julia Allen, Mark Ardis, Thomas Hilburn, Andrew Kornecki, Richard Linger, and James McDonald. *Software Assurance Curriculum Project Volume I: Master of Software Assurance Reference Curriculum* (CMU/SEI-2010-TR-005). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2010.
http://www.sei.cmu.edu/library/abstracts/reports/10tr005.cfm

[15] Mead, N., Hawthorne, E., & Ardis, M. (2011). *Software Assurance Curriculum Project Volume IV: Community College Education* (CMU/SEI-2011-TR-017). Retrieved March 26, 2013, from the Software Engineering Institute, Carnegie Mellon University website:
www.sei.cmu.edu/library/abstracts/reports/11tr017.cfm

[16] Mead, Nancy, Thomas Hilburn, and Richard Linger. *Software Assurance Curriculum Project Volume II: Undergraduate Course Outlines* (CMU/SEI-2010-TR-019). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, 2010.
http://www.sei.cmu.edu/library/abstracts/reports/10tr019.cfm

[17] www.theiet.org/policy/thought-leadership/cyber-security/

[18] Common Weakness Enumeration. A Community-Developed Dictionary of Software Weakness Types. *2011 CWE/SANS Top 25 Most Dangerous Software Errors.*
http://cwe.mitre.org/top25/

[19] The Open Web Application Security Project (OWASP). Top Ten 2013 Project: The Ten Most Critical Web Application Security Risks.
https://owasp.org/index.php/Top_10_2013_T10

[20] Cooper, S., Nickell, C., Perez, L., Oldfield, B., Berynielsson, J. Gokce, A., Hawthorne, E., Klee, K., Lawrence, A., and Wetzel, S. *Towards information assurance (IA) curricular guidelines*. In Proceedings of the 2010 ITiCSE working group reports (ITiCSE - WGR '10, Alison Clear and Lori Russell Dag (eds)). DOI=10.1145/1971681.1971686.

[21] Ibid.

[22] Kissel, R. ed. National Institute of Standards and Technology (NIST). *Glossary of Key Information Security Terms*. February 2011.
http://csrc.nist.gov/publications/nistir/ir7298-rev1/nistir-7298-revision1.pdf

[23] Ibid.

[24] Perez, L.C., Cooper, S., Hawthorne, E.K., Wetzel, S., Brynielsson, J., Gocke, A.G., Impagliazzo, J., Khmelevsky, Y., Klee, K., Leary, M., Philips, A., Pohlmann, N., Taylor, B., Upadhyaya, S. *Information Assurance in Two- and Four-Year Institutions*, in Proceedings of the 2011 ITiCSE Working Group Reports. Meeting held in Darmstadt, Germany, June 2011. Published by ACM 978-1-4503-1122-9/11/06

[25] Ibid. #21. p.40

[26] Ibid. #21. p. 51.

[27] National Cybersecurity Workforce Framework, published by NICE, February 2013. e
http://csrc.nist.gov/nice/framework/

[28] Ibid. #19.

[29] Frinke, D. Bishop, M. ACM *Curricular Guidelines Comments.* E-mail review of first draft of current report.

[30] Ironman document available at:
http://ai.stanford.edu/users/sahami/CS2013/ironman-draft/cs2013-ironman-v1.0.pdf

Feedback on CS2013 welcome through the Ensemble web portal:
http://www.computingportal.org/cs2013

[31] Ibid.

[32] Ibid. #3

[33] Ensemble web portal:
www.computingportal.org

[34] To read and share feedback on CS2013 through Ensemble, visit:
www.computingportal.org/cs2013

[35] http://www.cybersecuritycareers.com/