Cybersecurity Education Workshop

February 24 - 25, 2014

George Washington University Arlington Center

Arlington, VA

Final Report

April 7, 2014

Sponsored by the National Science Foundation Directorates of Computer & Information Science & Engineering (CISE) and Education and Human Resources (EHR) under CNS Award# 1428321

Executive Summary

In an effort to identify novel approaches to cybersecurity education, the National Science Foundation (NSF) Directorates of Computer & Information Science & Engineering and Education and Human Resources jointly sponsored a Cybersecurity Education Workshop, which was held February 24 & 25, 2014 at The George Washington University Arlington, VA Graduate Center.

The purpose of the workshop was to convene a diverse set of experts representing the computer science education (CS Ed), cybersecurity research, education and assessment, and industry communities in order to identify novel, compelling, and mutually beneficial approaches to advancing cybersecurity education. The recommendations resulting from the workshop will help guide the evolution of academic programs within the broad range of educational institutions.

Ideal State

Within a 5-year time frame, achieving the ideal state of undergraduate and graduate cybersecurity education in academia requires a multi-faceted approach. First, computer science programs should build security into the curriculum. Second, an interdisciplinary approach is needed to produce graduates with the needed abilities. Third, students need critical thinking, open-ended research projects, theory, grounding with practical problems, hands-on experiences, ability to learn and adapt to a changing world, ability to work effectively in teams and distributed teams, and oral and written communication skills. Fourth, we need a better understanding of the demand in the cybersecurity labor market. Anticipated demands in the labor market affect student choices and institutional decisions about academic courses, faculty and programs.

Research Themes and Recommendations

Six major research themes emerged from the workshop discussion. These themes should be considered within the context of a multi-disciplinary cybersecurity education environment. Although presented as separate themes, the lines between themes should not be seen as rigid boundaries. Rather, the themes and their associated recommendations should be considered as overlapping within the broad context of cybersecurity education. Recommendations for the role of NSF in advancing cybersecurity education to the ideal state are provided for each theme.

The six major themes and their associated recommendations are:

Concepts and Conceptual Understanding

Recommendation: The National Science Foundation should invest in research and curriculum development to close the gap between the definition and application of core concepts within and across disciplines by supporting initiatives that 1) define the core concepts that cybersecurity graduates at all levels (entry-level to leadership) should possess; 2) build consensus around the cybersecurity knowledge that should be integrated into the broad range of disciplines that contribute to cybersecurity education; 3) examine how well the core concepts translate across disciplinary boundaries and in inter-disciplinary contexts; 4) develop key learning outcomes and measurement instruments to assess student knowledge of those concepts; and 5) encourage cybersecurity educators at two-year and four-year colleges to collaborate with educational researchers to enable systematic investigations of educational innovation.

Educational Practice and Instructional Strategies

Recommendation: The National Science Foundation should invest in research projects that explore methods for balancing breadth and depth in cybersecurity education across interdisciplinary environments and for supporting the continuous evolution of curricular content. Specifically, NSF should invest in research that develops methods to quickly take new knowledge from research and incorporate it into the classroom. The ability to remove outdated content is as important as the ability to add new content. As the research community's understanding of topics improves, there should be a method to quickly remove obsolete content from courses. NSF should encourage the development of resources (eTextbooks and shared online resources are two possible methods) that support the rapidly evolving field of knowledge.

Recommendation: The National Science Foundation should invest in research that examines novel approaches to faculty development in a rapidly evolving field. The research should examine faculty development strategies for both research-oriented and teaching-oriented faculty members across the spectrum of educational institutions (e.g., 2-year, 4-year undergraduate and graduate) and should specifically address the relative impact of summer workshops, ongoing communities of practice, faculty externships in industry, social media, and mentoring. Summer workshops should focus on both cybersecurity content and educational research (co-led by experts in educational research).

Recommendation: The National Science Foundation should invest in projects that foster relationship building among faculty and computer security practitioners. These projects, such as faculty shadowing programs where faculty members leave campus and work along side practitioners, can catalyze cross-disciplinary interactions that support the development of stronger instructional materials.

Recommendation: The National Science Foundation should invest in research that focuses on cognition and instructional research in cybersecurity as advanced in the questions above. Specific topics should include the transformation of novices into experts, different educational needs for technicians versus professionals, and the effects of various instructional strategies on learning.

Shared Knowledge and Resource Development

Recommendation: The National Science Foundation should enhance existing efforts to build a central shared knowledge repository by supporting projects that examine 1) why previous efforts have been less than successful in maintaining content quality, participation, and sustainability; 2) the role that mobile technology and social media might play in enhancing participation; and 3) how to link such a repository to a larger community of practice.

Assessment

Recommendation: The National Science Foundation should invest in a program of research focused on the design of assessments in cybersecurity for advancement of cybersecurity learning. This research program should determine the efficacy of a variety of educational approaches, e.g., distance education options, hands-on labs and remote hands-on labs, competitions, collaborative learning and authentic learning experiences; and should explicitly encourage partnerships between educational research experts and cybersecurity educators.

Industry and Career Placement

Recommendation: The National Science Foundation should invest in studies that identify the greatest labor market demands in cybersecurity (federal, state, local and tribal government and private industry), including jobs that associate-degree graduates may be fully capable of performing.

Recruitment and Retention

Recommendation: The National Science Foundation should invest in research studies that investigate recruitment and retention in cybersecurity degree programs and the workforce. These projects should specifically focus on the recruitment and retention of women and other underrepresented groups in cybersecurity. In addition, NSF should encourage research into competitions and alternative activities including identifying and measuring the intended outcomes as well as finding ways to diversify the pool of those studying and pursuing careers in cybersecurity at various education levels.

Cybersecurity Education Workshop

Final Report

Introduction

In an effort to identify novel approaches to cybersecurity education, the National Science Foundation (NSF) Directorates of Computer & Information Science & Engineering and Education and Human Resources jointly sponsored a Cybersecurity Education Workshop[1]. The workshop, held February 24 & 25, 2014 at The George Washington University Arlington, VA Graduate Center, was organized by steering committee members Diana Burley (Co-chair, George Washington University), Scott Buck (Co-chair, Intel), Melissa Dark (Purdue University), Sue Fitzgerald (Metropolitan State University - MN), Elizabeth Hawthorne (Union County College), Tadayoshi Kono (University of Washington), and Stephen Portz (NSF).

The purpose of the workshop was to convene a diverse set of experts representing the computer science education (CS Ed), cybersecurity research, education and assessment, and industry communities in order to identify novel, compelling, and mutually beneficial approaches to advancing cybersecurity education.

This report provides an overview of the workshop and presents the major research themes and recommendations that emerged from the workshop discussion. The appendix at the end of this document includes the list of workshop participants, the workshop agenda, and the set of sample research questions generated by participants to guide future inquiries in the thematic areas.

Workshop Structure and Guiding Questions

The workshop was structured to maximize engagement and idea generation.

During the one and a half day workshop, the 24 participants representing the communities listed above generated a set of research themes in cybersecurity education, potentially laying the foundation for future research projects in this space. In addition, participants generated a set of actionable recommendations for future research on cybersecurity education and Computer Science education that support refined strategies for broadening participation in both communities.

The workshop was driven by a set of guiding questions that explored the ideal state of cybersecurity education, barriers to achieving the ideal state, cybersecurity education research gaps, educational research contributions, maintaining currency in curriculum, and industry-academia relationships. The specific questions posed within each of these

[1] CNS Award #1428321

categories are listed below:

- **Ideal state of cybersecurity education:** Within a 5-year time frame, what is the ideal state of undergraduate and graduate cybersecurity education in academia? How does your idea or the ideal state of cybersecurity education in five years differ from today? What do you see as significant barriers to achieving this ideal state?

- **Barriers:** What institutional, educational, and other barriers are preventing cybersecurity education adoption? As computer science, computer engineering, etc., grew what were the barriers to their growth? How can experiences gained in other fields be applied to cybersecurity education?

- **Cybersecurity education research gaps:** What aspects of cybersecurity education research are good candidates for attention? What are the emerging areas? In your opinion, what is missing and needs to be provided to inspire high quality cybersecurity education research? What notable advances in education research in other fields (Computer Science, Electrical and Computer Engineering, etc.) might apply to cybersecurity? How might this relate to what is missing and needs to be provided to inspire high quality education research in computer science, engineering, and other disciplines?

- **Educational Research Contributions:** In your experience, what are the top 1-3 factors/innovations that have impacted and improved student learning in your field? Of those, which may have relevance for cybersecurity education?

- **Curricular currency:** How can academia keep cybersecurity content current at various education levels?

- **Industry relationships:** What is the ideal relationship between academia and industry partners? How can partnerships or collaborations be fostered?

The section below highlights workshop participants' views on the ideal state of cybersecurity education and the barriers to achieving that state. Following this discussion, the major themes and associated recommendations that comprise the bulk of this report reflect the workshop discussion of the remainder of these guiding questions.

Multi-disciplinary Context

Cybersecurity is a multi-faceted problem that requires professionals with expertise in computing, law, finance, business, psychology, medicine, epidemiology, insurance, technology, public policy, and many others. By integrating cybersecurity content into the educational programs of multiple disciplines, graduates across the range of

cybersecurity professions will have the awareness and basic knowledge necessary to practice better personal cyber hygiene and to productively relate cybersecurity to their respective career fields. Both discussions – the ideal state, and the themes and recommendations – should be considered within the context of a multi-disciplinary cybersecurity education environment.

Ideal State and Barriers to Achieving that State

Within a 5-year time frame, achieving the ideal state of undergraduate and graduate cybersecurity education in academia requires a multi-faceted approach. First, computer science programs should build security into the curriculum by a) adding security concepts to introductory courses; b) supporting the integration of security concerns within advanced courses (e.g. systems analysis and design); and c) developing specific courses that address foundational security concepts across the broad spectrum of computer science topics. Second, and equally important, an interdisciplinary approach is needed to produce graduates with the needed abilities. Progress is needed in a) developing dedicated cybersecurity programs of study with standalone majors; b) integrating more cybersecurity content across the computer science curriculum; and c) integrating cybersecurity in several other disciplines, such as political science, business, management, law, finance, psychology, philosophy, math, history, etc. Third, students need critical thinking, open-ended research projects, theory, grounding with practical problems, hands-on experiences, ability to learn and adapt to a changing world, ability to work effectively in teams and distributed teams, and oral and written communication skill. Fourth, we need better understanding of the demand in the cybersecurity labor market; such data is useful for informing institutions about the number and type of degree offerings as well as the desired knowledge, skills, and abilities of graduates.

The expansion of graduates with a degree, certificates, professional certifications, minor or concentration in cybersecurity serves several key functions. First, it helps recruit prospective students to the field. Second, it provides a mechanism for prospective employers to hire capable and interested graduates. Third, it becomes a focus that prompts institutions to undertake curriculum review, which is a primary mechanism for ensuring the relevance and currency of content in degree programs. Finally, it allows for institutions to develop distinctive specialty areas; e.g., forensics, secure programming, risk analysis, etc. Cybersecurity requires not only good technology, but also good administrative and institutional processes. As dedicated cybersecurity programs are developed, it is critical that theories and principles from other relevant fields be included in the program of study. For example, incident response uses principles and theory from psychology that are needed in and easily transferable to a cybersecurity context.

In addition to dedicated cybersecurity programs, majors/minors, certificates, and concentrations, security classes cannot continue to be only electives in the computer

science programs, which allows computer science students to enter workforce with little-to-no knowledge or awareness of security issues, thus possibly contributing to security problems. Cybersecurity should be viewed as foundational knowledge in computer science, analogous to the manner in which other topics such as programming, operating systems, networking, computer architectures, etc., are viewed as fundamental topics.

Because of the pervasive nature of information technology, cybersecurity is permeating many fields, necessitating the integration of cybersecurity into various associated disciplines. Cybersecurity is a concern that draws professionals with expertise in computing, law, finance, business, medicine, epidemiology, insurance, technology and public policy, and many others. By integrating cybersecurity into other disciplines, more graduates will have awareness and basic knowledge needed to practice better personal cyber hygiene and to productively apply cybersecurity principles to their respective career fields.

Cybersecurity knowledge, like all knowledge domains, is more than a set of topics. The value of cybersecurity knowledge accrues in the translation of knowledge to practice. Cybersecurity is a rapidly changing field/landscape; this makes it challenging to provide graduates with a knowledge base that has a "long shelf life". It is critical that cybersecurity graduates have capabilities a) to learn and adapt to a changing world, b) to work effectively in teams and distributed teams, c) to think critically, and d) to communicate effectively. To produce graduates with these capabilities, cybersecurity education needs instructional research and development in several areas. Areas that have high potential for advancing educational research and practice in cybersecurity include the following:

1. Project-based learning, especially those based on real-world events, offer learners practical knowledge and makes them more employable.

2. Active learning methods and models that explore:

    a. How learners construct and conditionalize their cybersecurity knowledge; and

    b. Instructional methods for developing robust knowledge are particularly necessary.

3. Cooperative learning models and methods that enhance learners' abilities to acquire and utilize knowledge from multiple, varied, and distributed sources.

Finally, the ideal state of cybersecurity education will be served by enhanced understanding of the labor market. Key questions for which we currently have little understanding include: Where do graduates find work? What are the qualifications and skills in demand? What are the geographical and industry factors shaping the cybersecurity labor market? What are salient working conditions?

Barriers

Several barriers exist to realizing the "ideal state". The barriers include a lack of resources, lack of faculty knowledge and/or willingness to integrate cybersecurity content, the lack of flexibility to incorporate into other areas, lack of agreed standards or curriculum in cybersecurity education, and a lack of meaningful educational research in cybersecurity. Other barriers that exist for this field include a) time – increasing student knowledge may be longer than 4 years; b) assessment – the field is absent meaningful assessment instruments); c) institutional structures – there is not much understanding about cybersecurity from the perspective of administrators/other faculty/parents/students; finding a "home" for cybersecurity is difficult because it spans different departments, and d) institutional resources – not only are there territorial disputes within institutions over cybersecurity programs, there is also a shortage of institutional finances for beginning new programs.

The research themes described below can help to address the barriers and move cybersecurity education toward the ideal state.

Research Themes

Six major themes emerged as cybersecurity education research priority areas:

- Concepts and Conceptual Understanding
- Educational Practice and Instructional Strategies
- Shared Knowledge and Resources
- Assessment
- Industry and Career Placement
- Recruitment and Retention

Although presented as separate themes, the lines among themes should not be seen as rigid boundaries. Rather, the themes and their associated recommendations should be considered as overlapping within the broad context of cybersecurity education. For example, the development of key concepts provides a foundation for assessment. Below, each section provides an overview of the priority area and specific recommendations for resource investments. In making these resource decisions, the National Science Foundation should consider the balance between new investments and sustaining existing projects with promising results through renewable funding opportunities.

Concepts and Conceptual Understanding

According to Bloom's taxonomy, "conceptual knowledge is knowledge of classifications, principles, generalizations, theories, models, or structures pertinent to a particular disciplinary area."[2] Conceptual understanding refers to an integrated and functional grasp of given classifications, principles, generalizations, etc…[3] Conceptual understanding means knowing more than isolated facts and methods to include knowing why and when an idea is important, and the contexts in which is it useful. Conceptual understanding suggests that the knowledge is organized into a coherent whole, which facilitates learning new ideas by connecting those ideas to what is already known.

Despite the multitude of efforts initiated by the NSF, the National Institutes of Standards and Technology's (NIST) National Initiative for Cybersecurity Education (NICE), and the NSA's Centers of Academic Excellence in Information Assurance Education Program to define a core body of knowledge (including core concepts) for cybersecurity education, a gap still exists in the definition and application of these fundamental principles within and across disciplines. Past efforts have focused on defining the knowledge, skills and abilities of prospective employees. However, of greater importance is the development of individuals who, while well-grounded in the fundamentals, can think critically, creatively solve problems and anticipate future developments.

Disciplinary learning outcomes based on those concepts essential for all cybersecurity graduates regardless of the specialization/host major need to be further developed and evaluated. These fundamental concepts constitute the essence of the discipline. Learning outcomes must be tied to the core concepts of the field. As these learning outcomes are developed, their applicability must be assessed using a variety of measures including the state of our national security, the rate of growth of data breaches and other security incidents, employer satisfaction with recent graduates, and the value recent graduates place on their educational experiences.

Cybersecurity is a multi-faceted, rapidly evolving field. Beyond the core of the discipline, the field will advance if we define curricular guidance and meaningful learning outcomes that make known what is expected of graduates from a reasonable set of two-year and four-year degree programs. Learning outcomes should be defined for students from different types of programs, e.g., what are the appropriate learning outcomes for a bachelor's degree in computer science with a cybersecurity concentration in cybersecurity in comparison to the learning outcomes for a bachelor's degree in information technology? Establishing these learning outcomes (criteria) enables the development and sequencing of courses and programs that are aligned to

[2] Anderson, L. W. and Krathwohl, D. R., et al (Eds.) (2001.) A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives. Allyn & Bacon. Boston, MA: Pearson Education Group

[3] Ibid

the criteria, and measurement instruments to assess student learning and program outcomes.

In addition to being proficient in disciplinary content, the field will advance if we define other criteria that are necessary for cybersecurity graduates. For example, critical thinking, the ability to work in teams, understanding of professional and ethical responsibility, all have been identified in various forums as needed skills for future cybersecurity professionals. If cybersecurity content is also to be integrated into other programs of study, it would be useful to articulate learning outcomes for the concepts to be spread across the curriculum.

> *Recommendation: The National Science Foundation should invest in research and curriculum development to close the gap between the definition and application of core concepts within and across disciplines by supporting initiatives that 1) define the core concepts that cybersecurity graduates at all levels (entry-level to leadership) should possess; 2) build consensus around the cybersecurity knowledge that should be integrated into the broad range of disciplines that contribute to cybersecurity education; 3) examine how well the core concepts translate across disciplinary boundaries and in inter-disciplinary contexts; 4) develop key learning outcomes and measurement instruments to assess student knowledge of those concepts; and 5) encourage cybersecurity educators at two-year and four-year colleges to collaborate with educational researchers to enable systematic investigations and utilization of educational innovation.*

Educational Practice and Instructional Strategies

The interdisciplinary nature of cybersecurity cannot be overstated and cybersecurity degree programs should be taught in an interdisciplinary manner so that students who obtain a degree or specialization in cybersecurity acquire needed exposure to critical topics in law, finance, business, psychology, etc. Cybersecurity concepts should be integrated across the curriculum and within dominant fields, such as computer science, security courses should move out of the elective track and into mainstream requirements as described in ACM/IEEE Computer Science Curricula 2013[4].

The relatively new and rapidly evolving cybersecurity field has significant implications for the role of the faculty. First, professional development of faculty is imperative. Cybersecurity faculty members need ongoing professional development to ensure they are aware of and teaching the most current and relevant content. Faculty in disciplines where cybersecurity is to be integrated also need professional development that introduces them to the field and partners who can assist curriculum development and content integration. A second important topic with regard to faculty is the utilization of

[4] Report available: http://www.acm.org/education/CS2013-final-report.pdf

practice-oriented faculty, which includes faculty with practical experience in the field who are able to convey material in the context of the cybersecurity landscape.

Despite strong interest in projects dealing with curriculum development, assessment and evidence-based practices, most cybersecurity faculty members lack a solid grounding in educational research.

> *Recommendation: The National Science Foundation should invest in research projects that explore methods for balancing breadth and depth in cybersecurity education across interdisciplinary environments and for supporting the continuous evolution of curricular content. Specifically, NSF should invest in research that develops methods to quickly take new knowledge from research and incorporate it into the classroom. The ability to remove outdated content is as important as the ability to add novel content. As the research community's understanding of topics improves, there should be a method to quickly remove obsolete content from courses. NSF should encourage the development of resources (eTextbooks and online shared materials are two possible methods) that support the rapidly evolving field of knowledge.*

> *Recommendation: The National Science Foundation should invest in research that examines novel approaches to faculty development in a rapidly evolving field. The research should examine faculty development strategies for both research-oriented and teaching-oriented faculty members across the spectrum of educational institutions (e.g. 2-year, 4-year undergraduate and graduate) and should specifically address the relative impact of summer workshops, ongoing communities of practice, faculty externships in industry, social media, and mentoring. Summer workshops should focus on both cybersecurity content and educational research (co-led by experts in cybersecurity and educational research).*

> *Recommendation: The National Science Foundation should invest in projects that foster relationship building between faculty and computer security practitioners. These projects, such as faculty shadowing programs where faculty members leave campus and work along side practitioners, can catalyze cross-disciplinary interactions that support the development of stronger instructional materials.*

Cognition, Instruction and Instructional Strategies

Cognition is the process by which the sensory input is verified, manipulated, utilized, extended, transformed, reduced, stored, retrieved, and used. Cognitive processing

includes the attention of working memory, comprehending and producing language, calculating, reasoning, designing, developing, performing, proving, problem solving, and decision-making. As advances are made to characterize the nature of cybersecurity knowledge, the field will be better positioned to undertake research on how learners acquire input (cybersecurity knowledge) and transform, verify, manipulate, reduce, extend, elaborate, store, recover and use the information. One possible area of focus would be an investigation of the mental models of novices and experts in cybersecurity. Relevant questions include: How does the evolution from novice to expert unfold in the context of cyber security? What are the stages? What are characteristics of novices and experts in the context of cybersecurity?

Another crucial area is studying the effects of various instructional approaches and strategies on learning. Cybersecurity education uses a fair amount of hands-on learning, project-based learning, collaborative learning, and competitions as learning events. However, little empirical work has been done investigating the effects of these various instructional strategies on learning, motivation to learn, persistence, retention of learning, and self-efficacy. Moreover, little empirical work has been done to examine the role of these educational strategies on different types of skill development – technical and critical non-technical skills such as critical thinking and environmental analysis. Possible questions include: To what extent are hands-on labs efficacious in preparing students for skills-based certification? What are the best ways to evaluate learning during hands-on educational activities? What are the effects of competitions on student learning, retention and motivation to learn? Is there a performance difference between homogeneous versus heterogeneous teams in cooperative learning? How do we teach to support the distributed cognition found in the workplace? Will we get different outcomes if we teach security after we teach coding as opposed to teaching it concurrently? How does learning multiple representations stimulate sensory processing, and what are the effects on the development of expertise? Questions that address potential gender-based differences and which build on the research conducted through the NSF Broadening Participation in Computing (BPC) program[5] might include: Do outcomes from cooperative versus competitive learning events vary by gender? Do the attitudes of males and females differ toward cybersecurity competitions and if so, how?

> *Recommendation: The National Science Foundation should invest in research that focuses on cognition and instructional research in cybersecurity as advanced in the questions above. Specific topics should include the transformation of novices into experts, different educational needs for technicians versus professionals, and the effects of various instructional strategies on learning.*

[5] The NSF Broadening Participation in Computing website (http://www.bpcportal.org/) provides access to existing research through the digital library.

Shared Knowledge and Resource Development

Given the nascent state of the field, educators continue to need enhanced mechanisms for sharing and leveraging educational resources, and findings. A centralized resource that provides support, knowledge, education and training would be an asset to the field. The resource should be easily accessible and usable. Faculty members also need support for a sustained and centralized community of practice and scholarship.

Workshop participants were aware that the NSF has sponsored numerous cybersecurity education projects but wished to locate course materials more easily. Although resources exist, there is a wish for a comprehensive list of materials that can be easily searched and evaluated. Additionally, those seeking further funding would find it useful to see what has already been funded and produced to avoid duplication of effort. An easily accessible shared knowledge repository is a critical foundational resource for advancing to the ideal state of cybersecurity education.

> *Recommendation: The National Science Foundation should enhance existing efforts to build a central shared knowledge repository by supporting projects that examine 1) why previous efforts have been less than successful in maintaining content quality, participation, and sustainability; 2) the role that mobile technology and social media might play in enhancing participation; and 3) how to link such a repository to a larger community of practice.*

Assessment

Assessment is the field that helps us "know what students know." With assessment information, instructors are able to provide focused assistance to students who need it, and provide grades certifying students' knowledge levels. With assessment information, instructors are able to make improvements to curriculum, and employers, parents, and prospective students are able to make judgments about the effectiveness of courses, methods, and programs. Educational assessments are comprised of three components: 1) a model of how learners represent knowledge and develop competence in the domain (see theme concepts and conceptual understanding, and section 3, cognition, instruction, and instructional strategies above), 2) tasks or situations that enable students' knowledge and performance to become manifest and perceivable, and 3) an interpretation framework for drawing inferences and conclusions from the performance evidence obtained. These can be thought of as the three legs of the stool – cognition, observation, and interpretation must be connected in order for the assessment to produce meaningful results.

One of the notable innovations in physics education has been the development and use of concept inventories. A concept inventory is a type of assessment that evaluates whether a student has an accurate working knowledge of a specific set of concepts such as force and heat. Instructionally, concept inventories are used to diagnose individual

and group understanding. Other types of assessment, including professional certification exams and standardized tests, can be useful instruments for measuring student learning.

> *Recommendation: The National Science Foundation should invest in a program of research focused on the design of assessments in cybersecurity for advancement of cybersecurity learning. This research program should determine the efficacy of distance education options, including remote hands-on labs and authentic learning experiences; and should explicitly encourage partnerships between educational research experts and cybersecurity educators.*

Industry and Career Placement

The cybersecurity educational spectrum includes a variety of pathways. Industry certifications, certificates, minors, and concentrations at the undergraduate and graduate levels all provide different options for career placement. A considerable amount of work has been done to date by NICE, OPM, DHS, NSF, NSA and others to identify career options within the federal government. However, there still exists some confusion over the proper alignment of educational options and career paths both within the federal, state, local and tribal government sectors and industry.

Placement data provide meaningful indicators about the demand side of the cybersecurity labor market. Anticipated demands in the labor market affect student choices and institutional decisions about academic courses, faculty and programs. . Further, industry demands and the needs of the federal, state, local and tribal governments differ substantially. Data linking educational outcomes to the labor market would provide useful information. Of specific interest are data pertaining to two-year graduates. Technicians from associate-degree programs may in fact be better qualified to perform specific job functions than those graduating from a more theoretical bachelor's or master's program.

> *Recommendation: The National Science Foundation should invest in studies that identify the greatest labor market demands in cybersecurity (federal, state, local and tribal government and private industry), including jobs that associate-degree graduates may be fully capable of performing.*

Recruitment and Retention

The field of cybersecurity lacks studies examining recruitment and retention of students in degree programs. Examples of timely questions include: How effective are various mechanisms (e.g., marketing materials, extra curricular programs, etc.) in attracting prospective students to pursue education in cybersecurity? What are the levels of

interest in cybersecurity careers based on gender and other demographic factor? Are there particular cybersecurity related jobs that are more attractive to women and underrepresented populations? Is cybersecurity a good option for attracting more females to computing related education/work? How can we better leverage community colleges to increase the number of students pursuing baccalaureate studies in cybersecurity? How can we better leverage 4-year programs to increase the number of students pursuing graduate programs in cybersecurity? What is the impact of success in entry-level cybersecurity courses on persistence in the major?

> *Recommendation: The National Science Foundation should invest funds in studies that investigate recruitment and retention in cybersecurity degree programs and the workforce. These projects should specifically focus on the recruitment and retention of women and other underrepresented groups in cybersecurity. In addition, NSF should encourage research into competitions and alternative activities including identifying and measuring the intended outcomes as well as finding ways to diversify the pool of those studying and pursuing careers in cybersecurity at various education levels.*

Conclusion

As a multi-disciplinary endeavor, cybersecurity education must address the learning needs of three distinct student populations – those who will be informed users of information systems; those who will design or build the systems; and future cybersecurity professionals who will be tasked with protecting the confidentiality, integrity, and availability of the information housed on the systems. Efforts to reach these different student groups will require administrative awareness and support of education efforts that span traditional institutional boundaries.

In addition to the specific recommendations provided above, the appendix includes a set of sample research questions that will provide an initial point of inquiry for future research in cybersecurity education. The questions are organized into eight categories: assessment, concepts and conceptual understanding, general STEM and cybersecurity, repositories, educational practice, instructional strategies, placement, and recruitment, retention and diversity. The categories mirror the priority areas with two slight refinements – general STEM and cybersecurity questions are separated from questions of conceptual understanding; and questions of educational practice and instructional strategies are listed separately. Taken together, the themes, recommendations, and sample research questions offered in this report provide insight on the development of novel, compelling, and mutually beneficial approaches to advancing cybersecurity education.

APPENDICES

Cybersecurity Education Workshop
February 24-25, 2014
The George Washington University – Arlington Center

Participant List

Attendee	Affiliation	Email
Valerie Barr	National Science Foundation	vbarr@nsf.gov
Scott Buck*#	Intel	scott.buck@intel.com
Diana Burley*#	George Washington University	dburley@gwu.edu
Melissa Dark*	Purdue University	dark@purdue.edu
Ron Dodge	United States Military Academy	Ron.Dodge@usma.edu
Kevin Du	Syracuse University	wedu@syr.edu
Sue Fitzgerald*	Metropolitan State University (MN)	sue.fitzgerald@metrostate.edu
Jeffrey Forbes	National Science Foundation	jforbes@nsf.gov
Elizabeth Hawthorne*	Union County College	hawthorne@ucc.edu
Tadayoshi Kohno*	University of Washington	yoshi@cs.washington.edu
Keith Marzullo	National Science Foundation	
Kara Nance	University of Alaska	klnance@alaska.edu
Irene Lee	Sante Fe Institute	lee@santafe.edu
Wenke Lee	Georgia Tech	wenke@cc.gatech.edu
James Lightbourne	National Science Foundation	
Michael Loui	University of Illinois	loui@illinois.edu
Casey O'Brien	National CyberWatch Center	obrien.casey@gmail.com
Patti Pace	Lockheed Martin	patti.pace@lmco.com
Shari Pfleeger	I3P	shari.l.pfleeger@dartmouth.edu
Victor Piotrowski	National Science Foundation	vpiotrow@nsf.gov
Jo Portillo	ISC2	jportillo@isc2.org
Stephen Portz*	National Science Foundation	sportz@nsf.gov
Alan Sherman	Univ. of Maryland, Baltimore County	sherman@umbc.edu
Ambareen Siraj	Tennessee Tech	ASiraj@tntech.edu
Cara Tang	Portland Community College	cara.tang@pcc.edu
Blair Taylor	Towson University	btaylor@towson.edu
Josh Tenenberg	University of Washington	jtenenbg@uw.edu
Scott Tousley	Department of Homeland Security	scott.tousley@hq.dhs.gov
Zach Tudor	SRI	zachary.tudor@sri.com
Claude Turner	Bowie State University	cturner.bowiestate@gmail.com
Paul Tymann	National Science Foundation	ptymann@nsf.gov
Jesse Versalone	Champlain College	jvarsalone@champlain.edu
Marisa Viveros	IBM	viveros@us.ibm.com
Mark Wolkow	National Security Agency	mmwolko@nsa.gov

*Steering Committee, #Co-chairs

Novel, Compelling, Mutually Beneficial Approaches to

Advancing Cybersecurity Education

Sample Research Questions

Generated by Cybersecurity Education Workshop Participants
organized by eight categories

Assessment
What would be fundamental cybersecurity concepts for a concept inventory?
Another way of measuring competence is to look at the students' ability to solve problems. What does it mean to "solve problems" in cybersecurity? How can that be measured?
Where is the problem solving? What is the meat of the discipline? Are there fundamental concepts? Do they lend themselves to measurable learning outcomes? For example, it should be easy to define a bank of skills and measure the students' ability to perform at those skill levels. But this seems platform-dependent and may suffice.
What outcomes do we want to measure?
How can we assess the skills that make you successful in one or more of the cybersecurity domains?
Competitions/ skills validation. What methods are needed for validating (any instructional/ assessment) strategy?
How do competitions evoke/develop distributed cognition?
What are the best ways to evaluate the effectiveness of hands-on labs?
How do we observe without intruding, and how do we instrument to measure?
What are the effects of simulation based learning on student engagement in learning and the development of self-efficacy?
Concepts and Conceptual Understanding
What are the non-technical outcomes we need? Teamwork, critical thinking, what else?

How does the amount of time the team is together affect cognitive and affective learning outcomes?
Can we define a set of transferable skills that will be needed regardless of the cybersecurity specialization?
How do we know we have the right set of knowledge, skills and abilities (transferrable)? And how do we test those in the real world?
What are the fundamental skills and knowledge that are to be spread across the curriculum? What are the pre-requisites for these? Are there constraints on sequencing?
People see entire the range of tasks as their job and have trouble chunking it/delegating less skilled tasks to others. How can we shift the perspective to respect all skills, and teach students the value of distributed cognition?
What do students learn as a result of integrating cybersecurity across the curriculum? How effective are integration efforts?
How does the evolution from novice to expert unfold in the context of cyber security? What are the stages? What are characteristics of novices and experts in the context of cybersecurity?
General STEM and Cybersecurity
What math skills are really required for cybersecurity positions?
What model for maintaining a repository or sharing materials is sustainable?
How do we maintain the focus on basic math and science education (critical thinking skills) while preparing students for cybersecurity jobs/career?
Repository
Shared course material repositories (not just cybersecurity issue) • How do teachers find, use, adapt, reject, … materials from these repositories? • What form do these need to take so that they are useful, findable, adaptable, … • In what disciplinary areas or areas of practice have these historically been successful?
What does it take to make repositories usable?
A lot of content – how can it be coalesced into one easily accessible resource? How do

you motivate a person or organization to maintain and rate materials?
Model – large institutions provide resources for use of smaller institutions
Can we call on non-profits or university libraries to host the repository?
What model for maintaining a repository or sharing materials is sustainable?
Are there other areas of practice where this has been successful?
Would a fee-based approach work? Similar to library model.
Educational Practice
What are barriers to integrating cybersecurity across the curriculum (and models for overcoming these)?
What are the best educational practices in cybersecurity education? Why is it working? How do we ensure the expansion and extension of best practice?
Does cybersecurity have unique issues from other computing disciplines?
How do we institutionalize the development and sharing of educational research?
How do we quickly move research achievements into cybersecurity curriculum, industry practice and feedback to researcher?
Instructional Strategies
What are the effects of competitions on student learning and motivation to learn?
Do the attitudes of males and females differ toward cybersecurity competitions and if so, how? And what are the effects of those differences? Do males and females learn differently during competitions? If so, how can such environments be designed to be inclusive of all?
Borrowing from learning sciences: External "artifacts of practice" • What are these for cybersecurity? • How do professional practitioners generate and use these? • How do students generate and use these?
Homogeneous or heterogeneous groups in cooperative learning? Is there a performance difference?
To what extent are current hands-on labs efficacious in preparing students for skills-

based certification?
A large body of cognitive science research shows that expertise is based on: a) large and complex set of representation structures b) large set of procedures and plans c) the ability to improvisationally apply and adapt those plans to each situation's unique demands. How do learning multiple representations and being fluent among them contribute the development of expertise? d) The ability to reflect on one's own cognitive processes while they are occurring. How do learning multiple representations and being fluent among them contribute the development of expertise?
Expert teams—How do we teach to support the distributed cognition found in workplaces?
Will we get different outcomes if we teach security after you teach coding as opposed to as you teach coding? (Inject security concepts along the way.)
How do real environments, virtual environments, and non-hands-on activities compare with respect to fundamental concepts in cybersecurity?
If students experience a cybersecurity (field trip, internship, set of labs, etc.), how does their conception of cybersecurity (opportunities, field, practice) change?
What has happened with other integration efforts, e.g. "computer ethics" and "writing across curriculum" historically?
How does learning multiple representations and being fluent among them contribute the development of expertise?
Do we really need teachers who are CISSPs to teach security?
Placement
How would the following activities impact employer perception on hiring new cybersecurity graduates (who need experience)? a) Having cybersecurity professionals involved in student projects b) Providing real-world projects to cybersecurity students
What job roles do cybersecurity competitions prepare people for?

Where are the greatest market demands in cybersecurity? This could be broken down by level of degree and/or by area of concentration, e.g., secure coding, forensics, etc.?
Where are the greatest market demands in cybersecurity? This could be broken down by level of degree and/or by area of concentration, e.g., secure coding, forensics, etc.?
What is entry level for cyber jobs?
How can we encourage better delegation so as to make entry-level jobs available?
What jobs are out there for 2-year, 4-year degrees?
How can help desk employees be transitioned into cybersecurity jobs? What skills are necessary
What is the background/path of people who were successful in cybersecurity careers?
Looking at openings for cyber positions, what are the requirements, how are they distributed, how many required a clearance, how are they distributed geographically.
What are the personality traits of cybersecurity professionals (e.g., Myers Briggs, Strengths Finder)? ISC2 could be asked to survey their members. Profile the range of cybersecurity professional roles.
What are the real greatest market demands for specific jobs (e.g., forensics)?
Recruitment, Retention and Diversity
Cooperative/ competitive/ “learning”, does the result vary across gender?
What experiences outside of the classroom do students self-identify as associated with interest in cybersecurity?
What are the levels of interest in cybersecurity across gender and demographics?
Are there particular cybersecurity related job roles that are attractive to women and underrepresented populations?
Are there roles that are attractive to women and minorities in cybersecurity and if so, which ones?
If we focus on skills (e.g., communication, cooperation), how could that be used to recruit women and minorities to create a more inclusive workforce?
What does it take to attract women into cybersecurity jobs? To attract women to the study of cybersecurity? To retain women in cybersecurity studies? To retain women in

cybersecurity jobs?
What are the basic demographic statistics of the cybersecurity workforce compared to computer (these statistics may already exist)? • # women/minorities in cybersecurity studies • # women/minorities in cybersecurity jobs
What are the basic demographic statistics that may already exist? The number of women in cybersecurity studies?
Can cybersecurity be re-marketed/packaged/messaged to young girls to attract them to the field of cybersecurity? Such as promoting social good of cybersecurity of protect and defend, as well as privacy issues.
Is cybersecurity are more viable track for attracting a broader student pool to computing compared to other areas, e.g., software engineering, theory, mobile, telecommunications, etc.?
Have the Snowden media leads had an impact on students' view of working in the cybersecurity industry?
How can we best leverage community colleges to attract students to the field of cybersecurity?
To what extent is persistence in cybersecurity contingent upon doing well in entry level courses?
How to make cyber attractive to kids?
Is diversity awareness different for professionals in CS?
Maybe diversity needs to be explained differently to computer scientists (pride in intelligence masks awareness of inherent bias).
Is there a field with good diversity? What can we learn from that? What can we learn from other cultures where women are better represented (e.g., India)?

Cybersecurity Education Workshop

Pre-Workshop Survey: Summary of Compiled Responses

February 15, 2014

Prior to the workshop, participants provided initial thoughts on key questions regarding cybersecurity education. Survey questions are listed below along with summary responses.

1. Ideal state of cybersecurity education: Within a 5-year time frame, what is the ideal state of undergraduate and graduate cybersecurity education in academia? How does your idea or the ideal state of cybersecurity education in five years differ from today? What do you see as significant barriers to achieving this ideal state?

Answers included an interdisciplinary approach which would produce capable students. Many reported the importance of the integration of cybersecurity topics (software assurance, ethics, risk, etc…), not only in computer science courses but across all disciplines, such as political science, business, management, law, finance, philosophy, math, history, etc. Security classes cannot stay as electives in the Computer Science programs as this allows Computer Science students to go into workforce with little-to-no knowledge or awareness of security issues, thus possibly contributing to security problems. Cybersecurity should be taught in all classes from the beginning of students' courses. We should approach cybersecurity education with a variety of programs that include: critical thinking, open-ended research projects, theory, grounding with practical problems, hands-on experiences, ability to learn and adapt to a changing world, and communication skills.

In order to offer the best recruiting pool, universities should have BS graduates with a minor or concentration in cybersecurity as well as community and technical colleges offering certificates or degrees in it. We need clearly defined academic pathways to jobs. There is a suggestion that it would be helpful moving cybersecurity courses from undergraduate to graduate programs. Technical and nontechnical components of cybersecurity should be covered in the curriculum. Teaching materials should be shared. Universities could hire professionals as adjunct faculty. We should support a joint effort between industry and academia (intern at same time as in cyber program/studies), similar to nursing/doctor program approach (allows students real-world experience and change to bring back to classroom/faculty, allowing change to happen quickly). There exists a need for more specializations in particular areas. We should be looking at a two-year timeline, not five, as everything changes quickly.

The barriers include: lack of resources, lack of faculty knowledge and/or willingness to integrate cybersecurity content, the lack of flexibility to incorporate into other areas and lack of agreed standards or national curriculum in cyber education. We use the market

to drive changes in curriculum and have accreditation issues. There exists a corporate culture of only hiring BS graduates from Computer Science students. Cybersecurity is not a Major in its own right for undergrads—mostly courses/programming is offered at the graduate level. We need more training for faculty and more grants offered for workshop leaders. It is possible to look to the evolution of Computer Science as a way to guide cybersecurity programming approaches (origins from multiple departments but merge/evolve into new one). We should have all two- and four-year institutions offer strong cybersecurity programs.

2. Cybersecurity education research gaps: What aspects of cybersecurity education research are good candidates for attention? What are the emerging areas? In your opinion, what is missing and needs to be provided to inspire high quality cybersecurity education research? What notable advances in education research in other fields (Computer Science, ECE, etc.) might apply to cybersecurity? How might this relate to what is missing and needs to be provided to inspire high quality education research in computer science, engineering, and other disciplines?

Almost all participants listed more projects and collaboration as well as cooperative group learning (versus individualistic/competitive learning) as being important. Some suggested using methods that reinforce collaboration, cooperation, and problem-based learning. At that level, many would like to have more involvement from community/technical college faculty and students as well as encouraging research partnerships between them and universities. Effective professional development strategies need to exist for faculty. Many would like to see increased participation and retention of women and under-represented minorities in the field. Looking to Universal Design for Learning principles in education could inform Computer Science and cybersecurity education, which might address diversity issues.

We need defined and increased outcome assessments to find out best pedagogical practices for student population, especially with increased distance education. Attention should be focused on practice-centered education and research for students. It is important to incorporate modeling (inclusive of threat and attack modeling), which provides students with hands-on applications and scenarios to practice the craft. There should be more work in virtual computing, networks, and training in lieu of practicing with real systems. Suggested learning practices: active learning, problem based learning, and an inclusive learning environment. Many would like to see pedagogy for engagement (traditional lecture versus peer instruction as the peer instruction has higher level of newer content). Students should be taught secure Computer Science so that they are able to perform well in their jobs (exposure to proactive design/development decisions mitigating against potential vulnerabilities). It would be helpful to have domain specific curriculum as well as inclusion of cybersecurity across curriculum (example models of stats and history). Also, faculty should work on developing concept inventories of their students (similar to the Force Concept Inventory

in physics education) that inform if the student has misperceptions about the information they think they know.

What is missing: Adequate funding for developing infrastructure and supporting professional development opportunities, a platform for sharing resources, and an integrated community of educators to share information and resources. Also missing are the faculty buy-in (efforts on faculty development and awareness), attention to secure coding (bad habits learned during research projects) and the enforcement of software assurance in assignment grading.

3. Educational Research Contributions: In your experience, what are the top 1-3 factors/innovations that have impacted and improved student learning in your field? Of those, which may have relevance for cybersecurity education?

There were many opinions on impact and improvement. Innovations included: Massive open online courses (MOOCs), flipping classrooms, and agility of the institution to adopt and incorporate emerging content (a private institution versus a state school). It is important to have accessible systems (virtualization) and institutional leveraging of them. In order to bring positive attention to the field, universities should encourage the use of cyber exercises and cyber competitions.

In order to integrate students: using more closed lab sessions instead of at-home time to mitigate lack of cohort/team effort, lack of instructor input, etc. Students need more new materials and new ideas. Faculty would like to see funding for upgrading labs/lab materials and technology tools that enable students to see or manipulate underlying mechanisms. For learning, suggestions included: 3-D simulation and virtual worlds, inspired, inquiry-based learning (not power points), using Socratic Method or inquiry-based approaches as well as student-generated content. Learning should be building on a solid basis of mathematical understanding and providing context by applying learned concepts to daily situations. There should be experiences designed for first-year students. Many faculty members would like to see widespread adoption of active and cooperative learning techniques. Also, learning support systems, such as Blackboard and Design to Learn can be better or more widely used. We need real world problem solving. Many would like to see service learning with interactive content and flexible teaching styles. Faculty could use psychometrics: concept inventories, or a type of multiple choice tests, to discover what students' preconceived ideas are coming into the learning experience (misconceptions versus complete ignorance).

We should encourage the inclusion of content and practice in the K-12 curriculum. Programs should have competency-based assessments. There is a desire for the ability to interact globally. We need to acknowledge distance education and its increase. Also, other factors for students: YouTube, Wikipedia, and social media. We can collaborate

with test beds that allow institutions with fewer resources to provide high quality test and lab environments formerly restricted to highly resourced institutions.

4. Barriers: What institutional, educational, and other barriers are preventing cybersecurity education adoption? As computer science, computer engineering, etc., grew what were the barriers to their growth? How can experiences gained in other fields be applied to cybersecurity education?

Barriers that exist for this field: 1) time (increasing student knowledge may be longer than 4 years); 2) awareness (increase program agility) because students with cybersecurity knowledge are a commodity, and 3) assessment (making necessary changes within programs and institutions for improvement). There exists an unequal access to technology. Universities need to use more informal educational strategies for educating and promotion (looking at practitioners' paths and comparing them) by looking at the industry.

Commonality is lacking and therefore preventing uniformity in adding new content to an already full curriculum. There is no broader availability of "complete curricula". Competent and current materials are insufficient: web-based materials versus textbooks (inconsistency versus not being up-to-date). We should look to using Computer Science field as an example for creation of a field (established curriculum guidelines and scholarly research). Cybersecurity must span disciplines and not just sit in Computer Science or engineering curricula; there is a lack of incorporation across disciplines—it should be automatically embedded and be required coursework. A problem for incorporation might be that other programming feels threatened. An active learning infrastructure does not exist. Possible resistance to new topics might be for fear of thinking something else must be removed. The curriculum is already overcrowded. It is difficult to deal with the bureaucracy to change curriculum, add materials, or make rapid changes.

It is possible to use "borrowed" faculty and train them, which has strengths (cross-disciplines) and weaknesses (lack of formal training). Faculty expertise and teacher certification is lacking. The main barrier is lack of qualified faculty to staff programs. There exists a lack of drawing in females into computing careers as well as a lack of new faculty within this field in general. Professional development opportunities for faculty are rare. Many faculty members fear teaching an unfamiliar topic. Within departments, there is a lack of faculty support. Also, tenure requirements discourage education research for something like cybersecurity.

There is not much understanding about cybersecurity (from the perspective of administrators/other faculty/parents/students). It is difficult finding a "home" for cybersecurity since it spans different departments. Not only are there territorial disputes within institutions over cybersecurity programs but there is a shortage of

institutional finances for beginning new programs. Institutions need a clear definition of cybersecurity on a national level. Both middle schools and high schools do not have quality CS courses.

5. Up-to-date content: How can academia keep cybersecurity content current? How can academia keep cybersecurity content current? What is the ideal relationship between academia and industry partners? How can partnerships or collaborations be fostered?

Almost all participants in the survey reported the most important thing for cybersecurity is the relationship between academia and industry for information exchange. Suggestions for building relationships included: faculty going to a company as temporary employee and industry going to university as adjunct faculty, co-teaching with faculty and industry experts through videoconferencing and other collaboration technologies, hiring practicing professors, and internships for both faculty and students with industry partners. Adjunct faculty could be asked to do internal department seminars to keep faculty up to date. There should be incentives for academia and industry collaboration. The industry could assist in identifying needs for a more prepared graduate workforce, thereby helping with curriculum.

Faculty members need more opportunities to keep their knowledge current and that content needs to be integrated into the curriculum. We should also be looking at what adding new things (mobile computing and computing platforms) do to secure design. Faculty should teach empirical evaluation methods. Another suggestion was that industry advisory boards assist with curriculum. The IP rights of students prevent some collaboration with industry. It is helpful to attend the annual Colloquium on Information Systems Security Education (CISSE) colloquium that includes industry, academia, and government, possibly modeling Consortium for Computing Sciences in Colleges (CCSC) and Association for Computing Machinery-Women (ACM-W) regional conferences for those with limited budgets and promotion of local partnerships. Universities could require one-year paid internships in between junior and senior years as well as require work experience prior to graduate school acceptance. Universities should encourage more content creation as well as means to verify content is good. We can use dynamic sources of information, collaboration projects (e.g. INSuRE, RAVE), and internships.

Cybersecurity Education Workshop
Agenda - DAY 1: February 24, 2014

8:30 AM	*Steering Committee meets at GWU*	GWA 613
9 – 10:15 AM	**Opening Plenary** *(with morning refreshments)* • Welcome, Opening Remarks (10 min) *Scott Buck – Intel/Steering Committee* *Keith Marzullo, James Lightbourne - NSF* • Workshop Objectives & Scope (10 min) *Victor Piotrowski - NSF* *Scott Buck – Intel/Steering Committee* • Participant Introductions (1 min self introductions by participants) (25 min) • Summary of survey responses (15 min) *Melissa Dark - Purdue/Steering Committee* • Charge for discussion groups (5min) *Melissa Dark - Purdue/Steering Committee*	GWA 613
	Transition to WG Session 1	
10:30 – 12 PM	**WG Session 1** *(4 groups of 6 people) Moderator: Beth Hawthorne* Small group discussion – Ideal state of cybersecurity education (50 ~~40~~ min) Discussion Questions • Reflect on the collective expression (from the summary survey results) of the ideal state of undergraduate and graduate cybersecurity education. What should the role of NSF be in moving academia toward this reality? • Many different lower and upper-division undergraduate and graduate programs will feed the broad cybersecurity workforce. Some of these programs are disciplinary based, others are not. How should NSF prioritize programmatic investments? • What other ideas does this discussion foster? Reconvene in GWA 613 (10 min) for Report out (40 min - 10 min/group)	GWA 611-Yellow GWA 612-Blue GWA 613-Red GWA 614-Green
12 – 1:30 PM	**Working lunch –** *Moderator: Scott Buck* ***Pick up box lunches outside GWA 613*** **Industry Roundtables** (Session 1 groups/rooms + Industry Rep) Discussion Questions (40 min) • What is the ideal relationship between academia and industry partners? [Y/R] • How can partnerships or collaborations be fostered? [R/B] • What are the biggest challenges industry is facing in the cybersecurity workforce? [B/G] • What innovations are occurring in cybersecurity education/training in industry that we need to be about/be aware of? [G/Y] Reconvene in GWA 613 (10 min) for Report out (40 min - 10 min/group)	GWA 611-Yellow GWA 612-Blue GWA 613-Red GWA 614-Green
1:30 – 1:45 PM	**BREAK**	

1:45 – 3:05 PM	**WG Session 2** *(4 groups of 6 people)- Moderator: Melissa Dark* Small group discussion - Maintaining currency and fostering innovation (40 min) Discussion Questions • What role can NSF play in assisting academic institutions maintain currency of cybersecurity curricular content? How can NSF foster relationships between industry and academia to support content updates and innovation? • How can NSF encourage the transfer of innovations from other fields and the development of new innovations in cybersecurity education? • How should NSF determine the appropriate balance between supporting new innovation and continuing to support existing projects? • What other ideas does this discussion foster? Reconvene in GWA 613 (10 min) for Report out (40 min - 10 min/group)	GWA 611-Yellow GWA 612-Blue GWA 613-Red GWA 614-Green
	Transition to WG Session 2	
3:15 – 4:45 PM	**WG Session 3** *(4 groups of 6 people)- Moderator: Sue Fitzgerald* Small group discussion – Identifying and overcoming barriers (40 min) Discussion Questions • Identify and categorize key institutional, educational and other barriers to advancing cybersecurity education. • How can NSF encourage transformational cybersecurity educational innovation in spite of the barriers? • What other ideas does this discussion foster? Reconvene in GWA 613 (10 min) for Report out (40 min - 10 min/group)	GWA 611-Yellow GWA 612-Blue GWA 613-Red GWA 614-Green
4:45 – 5:15 PM	Plenary – Summarize day, plan for evening and day 2 – *Moderator: Scott Buck*	GWA 613
5:15 – 6 PM	Break (Transition to Holiday Inn)	
6 – 8 PM	Working dinner – *Moderator: Melissa Dark* *Dinner will be served at 6PM* Conducting, translating and applying educational research; evaluation and assessment Homework Questions • How can NSF encourage institutions to conduct, translate and apply educational research in undergraduate and graduate cybersecurity education? • How should NSF prioritize investments in cybersecurity educational research? • Assessment can be used to evaluate students or programs, either formatively for purposes of improvement or summatively to render judgment/results at a point in time. In your view, what are the most substantive assessment needs in cybersecurity? • What other ideas does this discussion foster? • Identify the 3 key ideas from the day's discussion and provide comments from the perspective of your area of expertise	Holiday Inn – Arlington at Ballston
8:00 – 8:30 PM	*Steering Committee meets to discuss Day 2*	

Cybersecurity Education Workshop
Agenda - DAY 2: February 25, 2014

9 – 9:20 AM	**Opening Plenary** *(with morning refreshments)* Overview – *Moderator: Melissa Dark Scott*	GWA 613
	Transition to WG Session 4	
9:20-– 10:20 AM	**WG Session 4** *(Small groups – self-selected based on research interests)* • Generate research questions – individually • Discuss and refine research questions • Group facilitator to email generated list of research questions to cyberedworkshop@gmail.com	GWA 611-Yellow GWA 612-Blue GWA 613-Red GWA 614-Green
	BREAK	
10:30 – 10:40 AM	**Voting on research priorities**	
10:40 – 11:10 AM	WG Session 5 *(Small groups – self-selected based on research interests)* • How should NSF encourage institutions to conduct, translate and apply educational research in undergraduate and graduate cybersecurity education? • How should NSF prioritize investments in cybersecurity educational research?	GWA 611-Yellow GWA 612-Blue GWA 613-Red GWA 614-Green
11:10 – 12 PM	Closing Plenary - Discussion Large group – *Facilitator: Melissa Dark* • Results of vote • Report out Security micro grant program – *Facilitator: Scott Buck* Wrap up – *Facilitator: Sue Fitzgerald* Next steps • Send any notes or additional thoughts to cyberedworkshop@gmail.com by Wednesday • A draft of the report to the NSF will be sent out to the group the week of March 17-21 with a request for feedback within one week • Final report will be submitted to the NSF by the end of March Thank you for participating!	GWA 613
	WORKSHOP END	
12 – 1:30 PM	Steering Committee – Working lunch	GWA 612

Additional References

ACM/IEEE-CS Joint Task Force on Computing Curricula. (2013.) Computer Science Curricula 2013. ACM Press and IEEE Computer Society Press. DOI: http://dx.doi.org/10.1145/2534860

Cooper, S., Nickell, C., Pérez, L., Oldfield, B., Brynielsson, J., Gökce, A., Hawthorne, E., Klee, K. Lawrence, A., and Wetzel, S. (2010.) "Towards information assurance (IA) curricular guidelines." Proceedings of the 2010 ITiCSE working group reports, ACM, New York, NY: 49-64. DOI: 10.1145/1971681.1971686

Cooper, S., Nickell, C., Piotrowski, V., Oldfield, B., Abdallah, A., Bishop, M., Caelli, B., Dark, M., Hawthorne, E., Hoffman, L., Pérez, L., Pfleeger, C., Raines, R., Schou, C., and Brynielsson, J. (December 2009.) "An exploration of the current state of information assurance education", ACM SIGCSE Bulletin, v. 41, no. 4, ACM, New York, NY: 109-125. DOI: 10.1145/1709424.1709457

ISC2 Common Body of Knowledge, Information Systems Security Certification Consortium, https://www.isc2.org/cbk/Default.aspx (last accessed April 7, 2014)

McGettrick, A. (August 30, 2013.) Toward Curricular Guidelines for Cybersecurity: Report of a Workshop on Cybersecurity Education and Training, ACM, http://www.acm.org/education (last accessed April 7, 2014).

National Centers of Academic Excellence, National Security Agency, http://www.nsa.gov/ia/academic_outreach/nat_cae/ (last accessed April 7, 2014)

National Centers of Digital Forensics Academic Excellence (CDFAE) Program, DoD Defense Cyber Crime Center, http://www.dc3.mil/cyber-training/cdfae (last accessed April 7, 2014)

National Cybersecurity Workforce Framework, http://csrc.nist.gov/nice/framework/ (last accessed April 7, 2014)

Pérez, L., Cooper, S., Hawthorne, E., Wetzel, S., Brynielsson, J., Gökce, A., Impagliazzo, J., Khmelevsky, Y., Klee, K., Leary, M., Philips, Am., Pohlmann, N., Taylor, B., and Upadhyaya, S. (2001). "Information assurance education in two- and four-year institutions." Proceedings of the 16th annual conference reports on Innovation and technology in computer science education - working group reports ACM, New York, NY: 39-53. DOI: 10.1145/2078856.2078860

Shumba, R., Ferguson-Boucher, K., Sweedyk, E., Taylor, C., Franklin, G., Turner, C., Sande, C., Acholonu, G., Bace, R., Hall, L. (2013.) "Cybersecurity, women and

minorities: findings and recommendations from a preliminary investigation." Proceedings of the ITiCSE working group reports conference on Innovation and technology in computer science education-working group reports. ACM, New York, NY: 1-14. DOI: 10.1145/2543882.2543883