REPORT OF THE 1998 ANNUAL MEETING OF THE NATIONAL COLLOQUIUM FOR INFORMATION SYSTEMS SECURITY EDUCATION (NCISSE)

ABSTRACT: The 1998 Annual Meeting of the National Colloquium for Information Systems Security Education (NCISSE) was held 16-18 June 1998 at James Madison University. It was an opportunity for leaders from industry, government and education to meet to define requirements for information security education and to influence and encourage the development of information security curricula at the graduate and undergraduate levels in American higher education. This paper summarizes those discussions and the suggestions that evolved from them. These are significant suggestions for immediate activities that can be undertaken by industry, government and education and will be further articulated by the Colloquium over the next year.

KEYWORDS: information systems security, information security, information assurance, information security education, information security curriculum development.

Charles W. Reynolds
James Madison University
Harrisonburg, Virginia

(540)568-2760 (voice)
(540)568-2727 (fax)
reynolds@cs.jmu.edu

INTRODUCTION

The National Colloquium for Information Systems Security Education (a Society for Advancing Information Assurance & Infrastructure Protection) opened its 1998 annual meeting 16-19 June 1998 at James Madison University in Harrisonburg, Virginia, with the following suggestion and call for action:

- All aspects of our lives and all aspects of our social, economic and political systems are becoming increasingly dependent on our information and communications infrastructure.
- The security and assurance of our information and communications infrastructure is therefore a national priority.
- To address this, we need an information-literate work force that is aware of its vulnerability and an information professional that is knowledgeable of the "best practices" available in information security and assurance.
- To provide a literate work force and to prepare information professionals is the task of American Higher Education.
- To meet this priority, Higher Education must be informed of the knowledge, skills and attitudes to be taught in the general curricula and in the information curricula of its colleges and universities.
- And industry and government must understand their role in supporting Higher Education and not simply expecting Higher Education to be responsive and informed about information security and assurance.

The objectives of the National Colloquium for Information Systems Security Education are

- to bring together industry, government, and academia to define current and emerging requirements for information security education,
- to discuss future direction of information security education at the graduate and undergraduate level,
- to form an advisory group to act as a forum for continued communications,
- to encourage colleges and universities to teach information systems security courses in various curricula to meet the needs of 21st century consumers,
- to increase course offerings to meet the growing demand for information systems security professionals

The “Colloquium” IS NOT an “Annual Meeting”. The Colloquium HOLDS an annual conference. The Colloquium IS a LIVING ENTITY - 365 days a year - by the communications it fosters and the products it produces.

SUGGESTIONS FOR ACTION

This paper is a summary of the dialog that occurred over three days at the 1998 annual meeting of the Colloquium. Many suggestions were made for action for the next year and it is the task of the Colloquium to begin to refine these suggestions into deliverable leading to its next annual meeting.

The Colloquium web site at http://www.infosec.jmu.edu/ncisse contains more extended versions of the comments summarized here. The following suggestions were made for action by the various constituencies (government, industry, education) of the Colloquium over the next year.

What government/industry/education should jointly do:

- Develop standards for what information security professionals should know and be able to do. Perhaps there's more than one kind of information security professional.

- Information Systems Security as a field has not matured sufficiently to develop processes associated with performing specific job related tasks. Until the processes are identified and related to performance standards, effective standardized training cannot be designed. Core processes associated with job related tasks must be developed. For example, what are a systems administrator's information security responsibilities?.

- Develop credentials for skills (e.g. firewall administration), technology (e.g. Novell file servers), roles (security administrator).

- Develop standards or metrics for IT infrastructure security with heavy reliance on those for other more established infrastructure.

- Identify the role of "best practices" in the profession and address the question "whose best practices".

- Overcome resistance among information security to the standards of rigor and discipline that are expected of other professions.

What industry can do:

- Provide equipment, software, help with maintenance to educational institutions.

- Funding (what else is new…) for chairs, scholarships, etc

- Grants for curriculum development.

- More reciprocity: onsite training for university faculty to include retraining of faculty who have not previously worked in information security.

- More feedback directly to universities through corporate partnerships.

- Funded internships for students to work in the information security area.

- Support creation of Information Assurance accident database accessible but not attributable or trackable except by the trusted agent.

What government can do:

- Course development and sharing (NSA and NDU and DISA can post courses that are developed on web for others to use).

- Avoid the parochial mind-set of ‘what is best for DoD'.

- The nearly overwhelming projected gap between the demand for and the supply of individuals educated in infosecurity calls for major increases in block grand funding in the universities and the marshalling of many other training and educational institutions.

- Encourage development of university Centers on Infrastructure Protection modeled after Materials Centers sponsored by NSF and Transportation Centers sponsored by DOT

What the information security profession should do:

- Improved network among faculty with more conferences on information security, more web sites, more journals.

- Establishment a formal system of recognition for outstanding education programs.

What educational institutions can do:

- Increase programs with concentrations in information security and include security courses in core curricula of all college graduates.

- Expand teaching of "soft skills" including practical experience, communication, multidisciplinary teamwork, business sense, negotiation, and the history of professionalism?

- There is much to be learned from other fields such as material science in specific and safety and quality in general as the academic community faced similar demands for students trained differently than had previously been the case.

- Offer computer ethics courses in all curricula.

- Solicit guidance from accreditation organizations for appropriate placement of information security within curricula

- Include information security in systems engineering and reliability engineering curricula.

- Provide continuing educational programs for working professionals.

- Initiate outreach program to high schools in the area of information security.

- Attract women and minorities to the computer field

- Develop educational assessment in information security.

- Develop improved techniques for educational assessment.

What information security educators can do:

- Develop and share practical laboratory exercises in information security.

- Most people learn ethics at home, very early, through stories, songs, games, etc. What is the appropriate analog in the world of computing? Could we design computer games, for example, expressing a set of different (more appropriate) values? Educators could collaborate on the development of new games for K-12 education.

- Develop a place to share instructional materials, or a place to share pointers to instructional materials.

- Write more textbooks (especially on practical issues) .

What legal education can do:

- Help U.S. lawyers understand the information security.
- Technical side must understand legal issues
- Legal side must understand technical issues

Problems in the academic culture to overcome:

- Time required to obtain approval of new curricula
- Difficulty of obtaining buy-in from other traditional academic departments.
- Many publications in an area and expertise on topics is rewarded above general expertise and integration of knowledge areas. For full advancement in some areas, one is required to be a world-leader. Not that many areas!
- Academia measures accomplishments by peer-reviewed publications in journals. Conference publications do not count in some venues. This produces a strong bias towards research in mathematical and theoretical areas.
- Papers on qualitative results are not universally accepted.
- “Squishy” sciences not well accepted.
- Papers bridging areas are difficult to judge.
- Breaking results are difficult to publish in a timely fashion.
- Discussion of ethics or policy is anathema.
- Cross-disciplinary studies impinge on turf across schools and departments.
- Joint appointments present difficulties for evaluation and advancement.
- Students may also have problems in pursuing interdisciplinary degrees
- Cross-disciplinary materials do not sell as well as those devoted to a single area. Finding up-to-date cross-disciplinary materials is difficult. Sharing of critical resources is difficult in some cases.
- Implementing an interdisciplinary program is difficult because resources are allocated to discipline-based departments. No one department "owns" the interdisciplinary program. Faculty are not recruited to teach across disciplines or between departments

THE PROGRAM

The suggestions above are freely extracted from presentations made at the annual meeting of the Colloquium whose program is shown below. The contributions of the speakers and all participants in generating the suggestions above is acknowledged and appreciated.

Invited Speakers

Critical Foundations Protecting America's Infrastructures.
Mr. Robert "Tom" Marsh, Chairman, PCCIP

Information Systems Security Education: The Needs of the Corporate World.
Dr. Jeffrey Jaffe, Vice President, Technology, IBM

What Everyone Should Know About Information Warfare & Assurance
Dr. Dorothy Denning, Professor, Georgetown University

Teaching the Big Picture of INFOSEC
Dr. Gene Spafford, Professor, Purdue University

Government and Private Sector Perspectives in Infrastructure Protection
Dr. William Harris, Commissioner, PCCIP

INFOSEC Education for Law Enforcement: An FBI Perspective
Mr. Ken Geide, Chief of Computer Investigations, FBI

Panels

Current Trends in Industry in INFOSEC Tools and Techniques.
Moderator: Ms. Gale Meyer, IBM
Panelists:
"Think Architecture First; Not Technology and Products"
Mr. Charles Blauner, JP Morgan
"Information Security Tools and Techniques"
Mr. Sam Phillips, Nations Bank
"Internet Security; Who Do You Trust?"
Mr. Alan Bender, Unisys Corp.

Meeting Security Requirements for Global Commerce: Can Education Help?
Moderator: Dr. Cynthia Irvine, Naval Post Graduate School

Federal Standards for INFOSEC Training.
Moderator: Dr. Vic Maconachy, NSA and Mr. Mark Wilson, NIST
"National Training Standards Workshop"
"NSTISSI Standards Worksheet"

The Academic Perspective: What Works and What Doesn't
Moderators: Dr. Debra Frinke, University of Idaho
Dr. John Cordani, James Madison University

Information Assurance
Moderators: Dr. Fred Giessler, National Defense Agency
Dr. William Harris, PCCIP
Dr. Todd Gooden, Office of the Joint Chiefs of Staff
Mr. Jeff Gaynor, Defense Information Assurance Program
Mr. Gary Sharp, Aegis Research Inc.

Discussion Sessions:

How can industry be encouraged to enhance the INFOSEC skills of employees through education?
Ms. Gale Meyer, IBM

Industry and government are strongly interested in influencing higher education to bring INFOSEC into the curriculum. What is needed from industry and government for higher ed to be responsive to this interest?
Dr. Cynthia Irvine, Naval Post Graduate School

How can higher education meet the needs of the INFOSEC professional for ongoing education without career interruption?
Dr. Karen Forcht, James Madison University

Teaching the social ethics of computing: Internet regulation or Internet anarchy?
Dr. Ming Ivory, James Madison University

Is INFOSEC inherently interdisciplinary? How can an interdisciplinary study by built into the existing structure of American undergraduate education? What undergraduate majors might find interdisciplinary INFOSEC courses appealing?
Dr. Marie Wright, Western Connecticut State University

What are effective design and delivery techniques for INFOSEC training?
Mr. Mike Lesley, Universal Systems, Inc.

THE HISTORY OF THE COLLOQUIUM

The National Colloquium for Information Systems Security Education (a Society for Advancing Information Assurance & Infrastructure Protection) was first formed in 1997 and was chartered this year at its second annual meeting. Quoting from its charter,

> All aspects of our lives and all aspects of our social, economic and political systems are becoming increasingly dependent on our information and communications infrastructure. The security and assurance of our information and communications infrastructure is therefore a national priority. To address this, our nation needs an information-literate work force that is aware of its vulnerability, as well as a cadre of information professionals that are knowledgeable of the recognized “best practices” available in information security and information assurance, as called for in Presidential Decision Directive 63, May 22, 1998.
>
> It is the task of American higher education to provide that information literate work force and to prepare information professionals. To meet this priority, higher education must be informed of the knowledge, skills and attitudes to be taught in the general curricula and in the information curricula of its colleges and universities. Industry and government must understand their role in supporting higher education, not simply expecting higher education to be responsive and informed about information security and assurance.
>
> The National Colloquium for Information Systems Security Education (the Colloquium) is established to serve as a living body to bring government, industry, and academia together to meet those challenges.

Quoting further from the Mission Statement of the Colloquium

> The Colloquium provides a forum for dialog among leading figures in government, industry and academia to work in partnership to define current and emerging requirements for information security education, and to influence and encourage the development and expansion of information security curricula especially at the graduate and undergraduate levels.

The first annual meeting of the National Colloquium for Information Systems Security Education was held on 23-24 April 1997 in Linthicum, Maryland. Expectations were far exceeded by the enthusiastic participation of prominent individuals in the field of information systems security (information security.) The profile of participants was well balanced from business and industry, from education, and from government.

The 1997 Executive Committee included
William V. Maconachy, National Security Agency, Chair
William H. Murray, Deloitte & Touche LLP
Corey D. Schou, Idaho State University
Frederick Tompkins, Information Systems Security Association
Barbara E. Prettyman, Allied Signal, Executive Secretary

The second annual meeting of the Colloquium was held 16-18 June 1998 at James Madison University in Harrisonburg, Virginia. Again the participation included many national leaders in information security education.

The 1998 Executive Committee was
Charles W. Reynolds, James Madison University, Chair
Matt Bishop, University of California-Davis
Dorothy Denning, Georgetown University
Kenneth Geide, Federal Bureau of Investigation
Frederick Giessler, National Defense University
Cynthia Irvine, Naval Post-Graduate School
Walter Jablonski, Defense Intelligence Agency
S. Kathleen Kincaid, IBM
William V. Maconachy, National Security Agency
William Murray, Deloitte & Touche, Inc.
Daniel Ryan, Science Applications International Corporation
Corey Schou, Idaho State University
Eugene Spafford, Purdue University
Allan Berg, James Madison University, Executive Secretary

The 1999 Executive Committee for next year is
S. Kathleen Kincaid, IBM, Chair
Matt Bishop, University of California-Davis
Dorothy Denning, Georgetown University
Kenneth Geide, Federal Bureau of Investigation
Frederick Giessler, National Defense University
William Harris, Former Commissioner, PCCIP
Cynthia Irvine, Naval Post-Graduate School
Walter Jablonski, Defense Intelligence Agency
William V. Maconachy, National Security Agency
Gale Meyer, IBM
William Murray, Deloitte & Touche, Inc.
Charles W. Reynolds, James Madison University
Daniel Ryan, Science Applications International Corporation
Corey Schou, Idaho State University
Eugene Spafford, Purdue University
Mark Wilson, National Institute of Standards and Technology
Allan Berg, James Madison University, Treasurer
Arlee Beckerdite, James Madison University, Executive Secretary