

A Study Of Security Education In The Era Of Cyber-Terrorism

James P. Lawler, (Email: JLawler@Pace.edu), Pace University
Zheng Li, Pace University
Yvette De Leon, Pace University

ABSTRACT

Cyber-Terrorism continues to confront the country with security threats. Since the September 11 attack, academia has not fully implemented in educational offerings a deterrence strategy satisfactory to the government. Though the National Security Agency has introduced Centers of Academic Excellence in Information Assurance Education, as an appropriate education program, there are only a small number of schools in the country that have enabled their offerings through this program. The focus of this study is to explore in survey the critical failure factors impacting the implementation of Centers of Academic Excellence education in academic institutions, by initially sampling schools in the Northeast Corridor of the United States. This study contributes to the discussion of important considerations for academic and governmental officials to further enable security strategy in this era of the cyber-terrorist.

“The United States must come to terms with ... cyber-security. We have enemies. They are smart. They will use our technology against us. They will attack the seams of our technology infrastructure. Our technology, like society, is ... interdependent. The only way to counter this threat is for ... government and [industry and academia] to work together.” – Richard Clarke, Former Special Advisor on Cyber-Security, White House Office of Homeland Security (Heiman, 2002)

BACKGROUND

The Internet benefits society. Domestically and globally, the Internet continues to enable improvement in the livelihood of citizens and their institutions. Economic, governmental and military infrastructures depend upon innovation that is expedited through cyberspace, the international network of interconnected systems and technologies on the World Wide Web of the Internet. Integration of banking, energy, health, telecommunication and transportation systems on the Web facilitates consumer and industrial interaction faster than earlier mechanisms of technology. The Internet is clearly critical in the efficient functioning of society in the 21st century.

The country however is challenged in the continued functioning of infrastructure systems and the Internet. Enemies are conscious of its dependency on the open connectivity of the Web. The National Research Council as early as 1996 indicated the growing reliance on vulnerable information infrastructures as “*the information security problem*” (Crowley, 2003). International terrorists are experts in sophisticated techniques that can attack the technological infrastructures of the country. Their tools can disguise a strategic threat costing trillions of dollars (Verton, 2002), as the techniques are not dissimilar from those exploited by casual culprits. The tools allow the threat of terrorists having the expertise of skilled hackers to be increased to substantial effect. The threat of an “*electronic Pearl Harbor*” (Webster, 1998) is considered heightened due to the physically destructive September 11 attacks on the World Trade Center and the Pentagon and those of the United States on terrorists in Iraq and Afghanistan (Kirkpatrick, 2002).

Efforts to secure key economic infrastructures from cyber-terrorism are not considered to be encouraging in the practitioner literature (Greenemeier, 2004, Petersen, 2004, Hunter & Mogull, 2003 & Sarkar, 2004). Studies indicate higher incidents of software flaws that have enabled increased hacker attacks and infrastructure downtime in 2004. These flaws have cost the economy almost \$60 billion (Hulme, 2004, page 54). Cyber-security is indicated to be costly and difficult to deploy, due to evolving technologies, and to be deficient in half of industry having not intrusion-prevention systems but mere intrusion-detection tools (Hulme, 2004, page 86). Government is noted to be negligent in not formulating integrated government and industry security strategy (Hulme, 2004, page 26 & Verton, 2004). Studies of the Meta Group indicate in an adapted Figure 1 that few firms in industry have excellent security strategy, irrespective of government. Given increased sophistication in threats and issues in implementing systems, further efforts in improving security strategy are important in defending the technological infrastructures of the country.

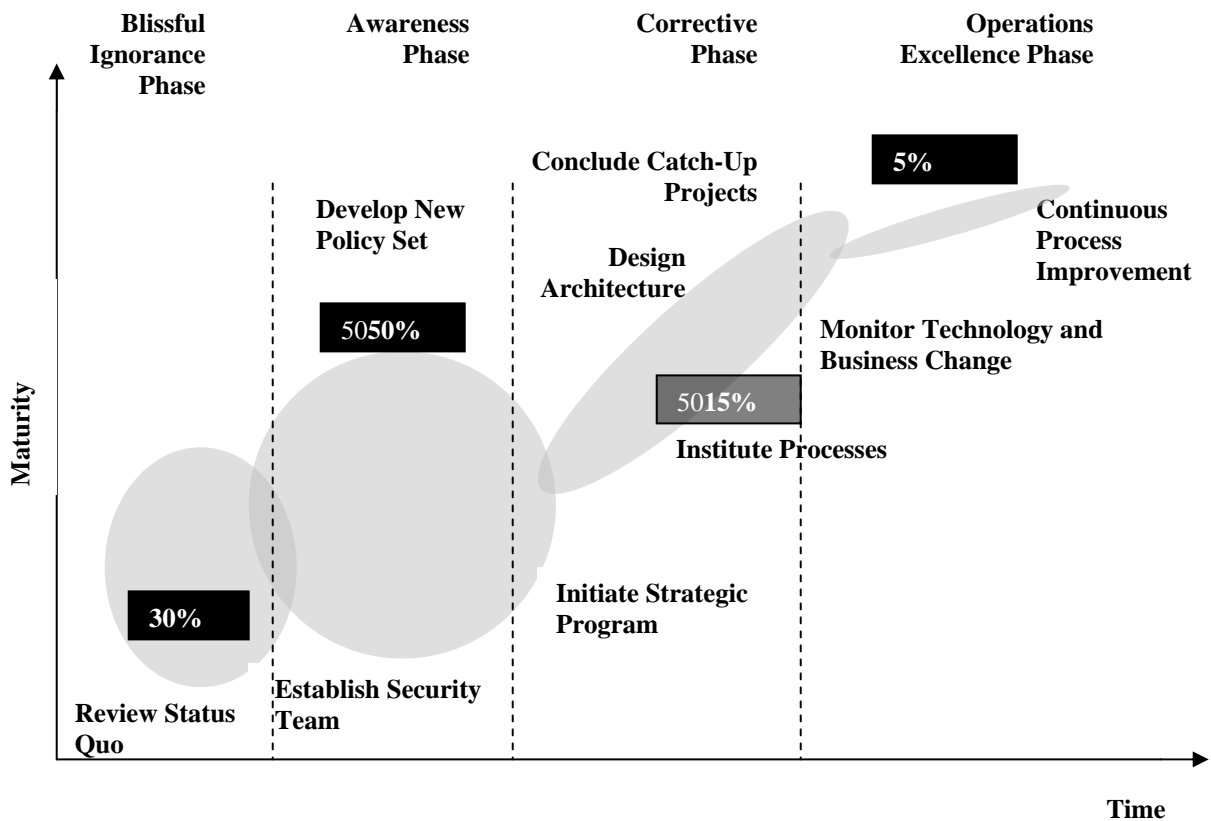


Figure 1: Information Security Market, 2004

Source: Meta Group, 2004

In launching the War on Terrorism in 2001, President Bush cited multidimensional efforts in defending the country (Roberto & Carioggia, 2002). Inclusion of security education from academia is important, but is not a frequently heralded initiative in this war (Berinato, 2003). Institutions have diverse engineering, information systems and computer science curriculum models integrating security education. These models may not be effective in a current cyber-terrorist security strategy. Programs often furnish more broad, core and theoretical learning and less practical, specific and time-to-exploit experience that links the learning to the external environment of security (Evans, 2003, page 6). Other limitations can include internal faculty not familiar with best government and industry practices in security strategy (Evans, 2003, page 12), out-of-date programs technologically (Bennett, 2004), and slowness in updating the programs (Evans, 2003, page 169).

Limitations in curriculum models may hinder security education in a time of increased sophistication of technologies and terrorist threats. Improvements in traditional models lag, due to daunting and lengthy internal procedures and external accreditation programs. The highly specific requirements of security limit linking of education models to market needs, than would be the case for generic skills (Evans, 2003, page 39). Skills of a security professional include an estimated 13 years of general technology experience, 7 years in security and several security related certifications, including Certified Information Systems Security Professional (CISSP) (Thibodeau, 2004). Not having taught graduates initial security skills needed by government and industry (Miller, 1997) is almost a threat to an efficient and effective information technology strategy (Datz, 2004, page 56), if not a security strategy. Such a threat necessitates a focused education strategy.

INTRODUCTION

A security education strategy is introduced in the Center of Academic Excellence in Information Assurance program, established by the federal government. This program is managed by the National Security Agency, in compliance with the Presidential Decision Directive 63 (PDD 63), on the National Policy on Critical Infrastructure Protection, of May 1998 (National Security Agency, 2004, Information Assurance Courseware Evaluation Program). The intent of the program is to lessen vulnerabilities of the country to cyber-terrorism by furthering undergraduate and graduate education in information assurance and by designating academic institutions that furnish this education. Information assurance is defined below:

“Information operations that protect ... information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.” (National Security Agency, Committee on National Security Systems [CNSS], NSTISSI 4009, 2004)

Center of Academic Excellence institutions are formally recognized by the National Security Agency, and students are aggressively recruited by industry and government if they have specific security skills learned in the program.

The Center of Academic Excellence program requires academic institutions to be compliant with criteria from standards of the National Security Telecommunications and Information Systems Security Committee (NSTISSC) (National Security Agency, 2004, National Information Assurance Education & Training Program). The criteria consists of Standard NSTISSI 4011 and one of NSTISSI Standards 4012, 4013, 4014 and 4015, as defined in Table 1 below:

Table 1: Center of Academic Excellence Standards

NSTISSI Standard	Definition
4011	National Training Standard for Information Systems Security (INFOSEC) Professionals
4012	National Training Standard for Designated Approving Authority (DAA)
4013	National Training Standard for System Administration in Information Systems Security
4014	National Training Standard for Information Systems Security Officers (ISSO)
4015	National Training Standard for Systems Certified [Staff]

Source: National Security Agency, National Information Assurance Education & Training Program, 2004

The criteria defined by the National Security Agency to evaluate the depth and maturity of curricula in information assurance in institutions is in Table 2 below:

Table 2: Center of Academic Excellence Criteria

Criteria / Category for Measurement	Source
Partnerships in Information Assurance Education	National Security Agency, Centers of Academic Excellence, 2004
Shared Curriculum	
Shared Faculty	
Reciprocity of Credits	
Information Assurance as a Multi-Disciplinary Science, Not a Separate Discipline	National Security Agency, Centers of Academic Excellence, 2004
Information Assurance as Modules in Existing Courses / Non-Technical Students Introduced to Information Assurance	
Information Assurance Concentration Programs in Non-Technical Courses	
Information Assurance Not Only in Teaching, but Encouraged as a Practice in University	National Security Agency, Centers of Academic Excellence, 2004
University or Departmental Information Assurance Security Plan	
Information Assurance Awareness Program for Faculty and Students	
University Information Systems Security Officer	
Research in Information Assurance Encouraged as a Practice in University	National Security Agency, Centers of Academic Excellence, 2004
Information Assurance Program with Dissertation, Thesis or Project Requirements	
Information Assurance Courses with Research Papers or Projects	
Non-Information Assurance Courses with Papers or Projects in Information Assurance	
Information Assurance Curriculum beyond Geographic Borders of University	National Security Agency, Centers of Academic Excellence, 2004
Information Assurance Curriculum Web Site	
Information Assurance Distance Education Technology	
Information Assurance Colloquia and Curriculum Workshops Sponsored by University	
Information Assurance Certificate Professional Studies Program	
Faculty Active in Information Assurance Practice and Research and Contributing to Information Assurance Literature	National Security Agency, Centers of Academic Excellence, 2004
Faculty Information Assurance Papers Published in Refereed Journals	
Faculty Information Assurance Education and / or Research Grants	
Faculty Information Assurance Presentations at Conferences	
State of the Art Information Assurance Library, References and Resources	National Security Agency, Centers of Academic Excellence, 2004
Availability of INFOSEC Educational Materials	
Availability of Historical Information Assurance Materials	
Declared Concentrations of Programs	National Security Agency, Centers of Academic Excellence, 2004
Information Assurance at Bachelor of Science Level	
Enrolled Students	
Graduated Students	
Information Assurance at Master of Science Level	
Enrolled Students	
Graduated Students	
Information Assurance at Doctorate Level	
Enrolled Students	
Graduated Students	
Declared Center for Information Assurance Education or Center for Information Assurance Research	National Security Agency, Centers of Academic Excellence, 2004
School Level	

University Level	
Full Time University Information Assurance Faculty	National Security Agency, Centers of Academic Excellence, 2004
Full Time Faculty with Information Assurance Program Responsibility	
Additional Full Time Faculty	
Intra or Inter Departmental or External University Shared Faculty	
Adjunct / Part Time Faculty	
Other University Information Assurance Education Partnerships *	Lawler, Li and De Leon, 2005
Partnerships with Universities and Schools	
Partnerships with State and / or Federal Agencies	
Partnerships with Corporations	
Partnerships with INFOSEC	
Partnerships with Trusted Products / Vendors	
University Other *	Lawler, Li and De Leon, 2005
Matriculated Information Assurance Students Employed in Security Positions	
Matriculated Information Assurance Students Employed in Corporate Security Positions	
Matriculated Information Assurance Students Employed in Government Security Positions	
Enrolled Information Assurance Students Employed in Security Internships	

These criteria were included in the study by the authors, in order to evaluate interactions with governmental and industrial institutions in a potential security strategy.

Institutions designated as Centers of Academic Excellence are required to be current in security education, and if current are re-designated Centers of Excellence in the third academic year. The National Security Agency evaluates its criteria to be current each year. Clearly, security education designed from criteria of the Center of Academic Excellence in Information Assurance program is a helpful, if not critical, component in fighting cyber-terrorism.

From an overall 1,800 institutions in the country, and 470 in the Northeast Corridor (U.S. News & World Report, 2004), there are only 59 as of February 2005 that are designated Centers of Academic Excellence in Information Assurance (National Security Agency, 2004, Centers of Academic Excellence – Institutions). The government program initiated in 1998. Though industry and government need graduates with specific security skills (Weinberger, 2004), non-Center of Excellence academic institutions may be limited in implementing a Center of Excellence model by historic inertia. Scholarly studies imply short perspective (Kim, Shim and Yoon, 1999) and slowness of faculty (Lightfoot, 1999, Maglitta, 1996 & Lee, Trauth & Farwell, 1995) in improving curriculum models important to industry. These studies indicate the importance of industry in helping institutions to update models (Srinivasan, Guan & Wright, 1999), though only a small number of institutions appear to be implementing immediate improvements in security education. The perception may be that non-Centers of Academic Excellence are not fully cognizant of the cyber-terror threat.

The reality is that academic institutions that include computer science, engineering and information systems schools are affected by an evolution in the field security education. Computer science and information systems are impacted by a new definition of information assurance, as both a technology and a process management discipline (Kahan, 2004). The evolving frame of reference of specific security skills needed by industry and government in a counter cyber-terrorism strategy is new to these departments. Practitioner studies indicate that non-Center of Academic Excellence institutions are implementing new education and skill models (Thurrott, 2004), but the models are frequently that of including a few courses in information security (Whitman & Mattord, 2004), not that of

improving curriculum programs (Kahan, 2004). Such limited models can benefit from Center of Academic Excellence in Information Assurance standardization.

Issues in the limitations of current non-Center of Academic Excellence models of institutions may be in factors that hinder compliance to Center of Excellence standards. Studies indicate the difficulty of faculty not having knowledge requirements in information security in initiating a Center of Excellence model (Kahan, 2004). Other issues may be in a need for funding, and for further guidance, by the National Security Agency in helping non-Center of Excellence institutions, or in a possible need for flexibility in the Center criteria and NSTISSC standards. Study of the failure of non-Center of Excellence institutions in specific Excellence requirements may enable improvement in the security education strategy of these institutions and subsequent initiative in the Center of Excellence program. Educational systems that cultivate the specific requirements of information security increase the likelihood that students will have the skills to confront cyber-terrorism (Irvine, Chin & Frincke, 1998).

FOCUS OF PRELIMINARY STUDY

The focus of the study is to explore the importance of Center of Academic Excellence criteria factors perceived as contributing to the small number of academic institutions designated Centers of Excellence in Information Assurance. Though institutions already designated Centers of Excellence enable analysis of success factors, analysis of potential failure factors in non-Centers of Excellence having charters in information systems and computer science education furnishes fresh insight that can help the latter institutions in planning for designation. The study is initiated in Accreditation Board for Engineering and Technology (ABET) institutions in the Northeast Corridor of the country, a key hub of information infrastructures that can benefit from improved security. Non-Center of Excellence ABET institutions in general in this region continue to enhance their curricula in security technology. Research is limited in the impact of the effectiveness of their programs in an eventual Center of Academic Excellence strategy.

RESEARCH METHODOLOGY

The research methodology of the current phase of the study consisted of an analysis of a sample of non-Center of Academic Excellence ABET institutions in states of the Northeast Corridor of the country. (The study originated in a competitive analysis of the security curricula of institutions by the School of Computer Science and Information Systems at Pace University, in New York City, in July – September 2003. The analysis was performed in conjunction with the application of the university to be a Center of Academic Excellence in Information Assurance. The National Security Agency approved the application in 2004.) The institutions in this study have had information systems, engineering and / or computer science schools since 1985. Total faculty in the institutions is from 3,400 to 320 full-time and from 810 to 25 part-time. Total students are from 28,100 to 2,150 undergraduate and from 12,100 to 150 graduate and post-graduate. The study included private and public institutions in two stages of analysis.

In *stage 1* of the study, a sample of 56 non-Center of Excellence ABET institutions were identified by the authors, in January – March 2004, based on the reputations of the schools as advanced in technology curricula. The content of catalog and descriptive information of undergraduate, graduate, and post-graduate curricula, furnished by technology and non-technology departments of the institutions, was analyzed for inclusion of security education and environment features. Course descriptions, not titles, were analyzed in the stage. Information on the Internet sites of the schools was additionally evaluated in this stage. Other practitioner literature on the institutions, in publications such as U.S. News and World Report, was evaluated for indication of security education.

In *stage 2* of this study, 44 out of the 56 non-Center of Excellence ABET institutions in stage 1 responded to a survey by the authors, in April – October 2004, on conformance of security education and environment features to Center of Academic Excellence criteria. The institutions in this stage are confidentially indicated by state in Table 3 below. An average of three Deans, Associate or Assistant Deans, Chairs, or full time professors in the computer science, engineering or information systems schools, in each of the institutions, were surveyed independently and individually on the telephone by one of the authors. Surveys averaged one to three hours per respondent and were based on a checklist instrument of 41 Information Assurance criteria categories indicated in Table 2 of this study. The

content of the instrument was checked prior to the survey by an academic non-author who has expertise in Center of Excellence certification and security education. (The checklist instrument is available upon request of the principal author.)

During stage 2, the authors confirmed conformance or non-conformance of Information Assurance in courses, modules in courses, and content in courses. They evaluated, where feasible, courses in the technology and non-technology curricula and programs of the institutions from selected syllabi and the survey. They further evaluated, where feasible, non-conformance or conformance to elements of NSTISSI 4011 – 4015 standards. To the category responses of the survey, the authors applied a simple 7-point rating scale from 6 – very high conformance to 0 – no conformance to Center of Excellence criteria, though not actual Excellence maximum or minimum numeric values due to the complexity of a more detailed evaluation. The quantitative data was exported by category to Excel, scored statistically in SPSS 11.5 by Excellence criteria in Table 2, and summarized by criteria by the authors.

**Table 3: Research Sample of Non-Center of Academic Excellence ABET Institutions
Northeast Corridor**

State	Private Institutions	Public Institutions	Total Institutions
Connecticut	2	3	5
Delaware	1	1	2
District of Columbia	1	2	3
Maine	1	1	2
Maryland	0	3	3
Massachusetts	4	1	5
New Jersey	2	2	4
New York	4	4	8
Ohio	1	0	1
Pennsylvania	5	2	7
Vermont	1	1	2
Rhode Island	2	0	2
Total	24	20	44

ANALYSIS

The analysis of the results of the survey disclosed low scores in all of the sampled institutions. Of the 44 institutions, only 13 had mean scores higher than 1.0 (very low conformance of Information Assurance). The analysis in Table 4 indicated higher closeness in conformance in overall scores in multi-disciplinary science (92.5 score), encouraged practice (80.3), education partnership (76.0), encouraged research (54.0), and state of the art resources (52.0). The other criteria for Centers of Excellence, in curriculum beyond borders (40.0), active faculty (18.7), full time faculty (10.8), other partnerships (9.8), other (6.7), concentrations of programs (0.0) and declared center (0.0), had lower conformance. The results deserve specific and generic comment.

As for generic comments, most of these institutions (37 / 44 schools) indicated low concern about Center of Excellence designation currently. Some (19) however indicated the eventual importance of Information Assurance in their curricula and environmental life. Some (11) have introduced Information Assurance in business schools. This latter focus, in beginning to conform to National Security Agency standards, is impacted by frequently indicated issues of other priorities (8) and resources (24): “*We have no current resources to offer these courses*”- Dean, Information Systems, Maryland Institution, 2004. Other issues included shifting of educational strategies that precluded review of Information Assurance by the schools at the time of the study (6).

As for specific comments, the institutions continued to have indication in Table 4 of efforts to enhance their Information Assurance curricula in multi-disciplinary science (92.5 score), encouraged practice (80.3), education partnership (76.0), encouraged research (54.0), and resources (52.0). Basic principles of Information Assurance, and project requirements and research, were included in modules of technology and non-technology courses. Evidence of

faculty practice and research (18.7), and of marketing of limited Information Assurance programs and workshops in diverse media (40.0), was sometimes indicated in the study. Nevertheless, the more critical Excellence determinants, of declared concentrations (0.0), declared center (0.0) and full time Information Assurance faculty (10.8), were discouragingly not in conformance in elements of NSTISSC standards, though not unanticipated by the authors. Interactions of the institutions with industrial and governmental institutions was also low in other partnerships (9.8) and other (6.7), with few of the institutions (11 schools) having records of graduated students in security related positions.

Encouraging from the results is that, irrespective of issues, the institutions that are more business focused (29 schools) and less liberal arts (15) in their curricula charters, and have mean scores higher than 1.5 (7), were indicated to be focused on becoming Centers of Excellence by 2008 or earlier. These institutions were indicated to be less public (1) and more private (6) schools, an indication highlighted in the Department of Commerce Study (Evans, 2003, page 79) that private schools are more flexible in modifying curriculum programs. For the latter institutions, Center of Excellence is a defined goal in their charters.

Further review of these results is needed in selected case studies, which will be finalized in mid-2005.

**Table 4: Analysis of Results of Non-Center of Excellence ABET Institution Survey
Northeast Corridor**

Criteria	Total Score	Score per School	Score per Category
Partnerships in Information Assurance Education	228	5.2	76.0
Information Assurance as a Multi-Disciplinary Science, Not a Separate Discipline	185	4.2	92.5
Information Assurance Not Only in Teaching, but Encouraged as a Practice in University	241	5.5	80.3
Research in Information Assurance Encouraged as a Practice in University	162	3.7	54.0
Information Assurance Curriculum beyond Geographic Borders of University	160	3.6	40.0
Faculty Active in Information Assurance Practice and Research and Contributing to Information Assurance Literature	56	1.3	18.7
State of the Art Information Assurance Library, References and Resources	104	2.4	52.0
Declared Concentrations of Programs	0	0.0	0.0
Declared Center for Information Assurance Education or Center for Information Assurance Research	0	0.0	0.0
Full Time University Information Assurance Faculty	43	1.0	10.8
Other University Information Assurance Education Partnerships	49	1.1	9.8
University Other	20	0.5	6.7

n = 44 Institutions x 41 Categories (12 Criteria)

IMPLICATIONS

“We have the role of playing Paul Revere and waking people up ... If cyber-war comes – and come it will – we want to be prepared. Why does it always have to be we do a great job after we are hit?” – Richard Clarke (Fisher, 2002)

The conflict between the conservatism of academic institutions and the demand of society for an effective security strategy is an important implication of this study. Non-Center of Academic Excellence information systems and computer science schools having curricula on principles of security, and not best practice applications relating to professional paths and skills (Spaford, 1998), are not fully helping industry and government. Inasmuch as security

skills are closely linked to ever changing software and hardware technologies, schools can be at a continued disadvantage in fighting cyber-terrorism. Practitioner studies indicate a lack of skilled specialists as an impediment to information security (Squire, 2003). Though institutions can be cognizant of this disadvantage (Roosevelt, 2005), efforts in enhancing curricula and programs are not considered fast enough (Carr, 2004).

The *importance of creativity, fastness and flexibility in improving security education strategy* is another implementation. Encouraging are internal initiatives, that include the Carnegie Mellon CyLab (Lindquist, 2004) and the Center for Information Assurance and Security (CIAS) at the University of Texas (Kelly, 2005), in implementing new security practices and technologies. External initiatives, that include Georgetown University, Northeastern University and the University of Pennsylvania, in innovating in information sharing and new security programs aligned with the International Security Management Association (ISMA) and AIS International, are helpful in models of security education strategy (Carr, 2004, page 13). Programs that include security executives in forums, such as the Information Technology Association of America (ITAA) and Business Software Alliance (BSA) (Fisher, 2003), and security professionals on faculty, can be helpful in improving education in Center of Academic Excellence criteria. Other informal programs that include faculty enhancing the education in consultation with chief security officers, and having students interface with security and business professionals in internships, can be helpful in academic institutions (Grimaila, 2004). Research centers initiated by academia (Ragatz, 2004) in conjunction with government and industry can enhance programs.

Further implications of the study include the *importance of funding for flexible security education strategy*. Investment in infrastructure security strategy is frequently limited in government and industry, due to economic constraints. Government incentives to academia in instruction, learning and research in new security practices and tools, and in securing hardware and software technologies, are however important in helping institutions conform to Center of Academic Excellence criteria (Berghel, 2003). Given the high criteria to be Centers of Excellence, the Department of Defense, the National Cyber-Security Division of the Department of Homeland Security, and / or the National Security Agency, could extend funding to financially limited non-Center of Excellence institutions, if they demonstrate efforts in improving security curricula and programs. Non-Center of Excellence information systems and computer science schools cannot be in isolation in the National Strategy to Secure Cyber-Space.

Implications include the *continued limited education of information systems and computer science graduates for positions as skilled security specialists*. Though the number of students in technology programs is lower in 2005 than in prior periods, non-Center of Academic Excellence institutions have in general not integrated Information Assurance in their curricula and programs in a differentiating and innovative manner. Initiatives of technology firms, such as CISCO (Grimaila, 2004), the new IBM Academic Initiative (King, 2004), Intel, Microsoft and Sun, can be helpful to institutions in integrating security technologies. Internships of information systems and computer science students in security positions in industry and government can also be marketable and timely (Mullin, 2004). The projections of a higher number of information technology positions, necessitated by government and industry through 2012 (Datz, 2004, page 58), includes security specialists (Gross, 2005) that have to be educated initially by academic institutions.

The final implication of the study is the *need for non-Center of Academic Excellence information systems and computer science schools to plan for security education that is sensitive to society*. Strategy has to consist of expanded military, government, health and other industry initiatives, as numerous infrastructure systems and technologies impact security in our society (Stahl, 2004). Security specialists in industry have to be immersed more in mitigating not internal application threats (Vijayan, 2004), but external infrastructure threats. Security education that is holistically included in both non-technology and technology disciplines is an effective enabler of a security strategy in society (McCreary, 2004). Such enabling implies further initiative is needed in non-Center of Excellence schools, and potentially from accreditation boards, such as ABET, in helping industry and government in an integrated security strategy that protects society.

LIMITATIONS AND OPPORTUNITIES FOR RESEARCH

The study introduced a framework for researching security education, as the small sample size of academic institutions in the Northeast Corridor furnished a limited basis for generalization to the population of ABET institutions in the country. The study included momentary investigations of several specific schools. The impact of these investigations, in a short time, may have limited significance and thoroughness, so that the implications of this study have to be filtered by the researcher. Further time in academic institutions, and in governmental and industrial organizations, planned by the authors in 2005, may improve future studies. Though this study focused on failure factors in Center of Academic Excellence criteria, a total study of the evolving field of security education strategy will have to include success factors.

CONCLUSION

This study of security education, in the initial sample of institutions in the Northeast Corridor, is insightful in factors inhibiting Center of Excellence in Information Assurance designation. Creativity and flexibility in the implementation of curricula and programs are important in enabling conformance to Center of Excellence standards. Government and industry help is also important in facilitating faster implementation of proactive programs. Further and broader research in the topic is needed in academic institutions throughout the country. The study furnishes a framework for continued research in education as a transformational force in security strategy.

ACKNOWLEDGMENTS

This study is funded by a research grant from the School of Computer Science and Information Systems (CSIS) at Pace University in New York City.

REFERENCES

1. Bennett, Cedric (2004) Scale the Solution to the Problem, *Educause Quarterly*, 1, 6.
2. Berghel, Hal (2003) The Discipline of Internet Forensics, *Presentation, Pace University*, New York, New York, October 31, 1.
3. Berinato, Scott (2003) The State of Information Security 2003, *CIO Magazine*, October 15, 1-3.
4. Carr, Kathleen S. (2004) Continuing Education, *CSO Magazine*, July, 13.
5. Carr, Kathleen S. (2004) Feather Your Nest, *CSO Magazine*, June, 2, 43.
6. Datz, Todd (2004) Degrees of Change, *CIO Magazine*, October 15, 56, 58.
7. Crowley, Dan (2003) Information System Security Curricula Development, Proceedings of the CITC4 2003 Conference, Lafayette, Indiana, October 16–18, 249.
8. Evans, Donald (2003) Education and Training for the Information Technology Workforce, *Report to Congress from the Secretary of Commerce, United States Department of Commerce*, June, 6,12,39,79,169.
9. Fisher, Dennis (2003) Executives Set Up Task Force, *eWeek*, November 17, 34.
10. Fisher, Dennis (2002) How Real Is the Threat?, *eWeek*, August 19, 21.
11. Greenemeier, Larry (2004) Step Up in Security, *Information Week*, October 25, 53.
12. Grimaila, Michael Russell (2004) Maximizing Business Information Security's Educational Value, *IEEE Security & Privacy*, January / February, 56-57.
13. Gross, Grant (2005) Security Jobs on the Rise, *CIO Magazine*, January 1 - December 15, 16.
14. Heiman, Don (2002) Public Sector Information Security: A Call to Action for Public-Sector CIOs, *National Association of State Chief Information Officers*, October, 4.
15. Hulme, George V. (2004) Losses from Viruses Reach Five Year High, *Information Week*, October 25, 86.
16. Hulme, George V. (2004) Under Attack, *Information Week*, July 5, 54.
17. Hulme, George V. (2004) Senator Criticizes United States Cyber-Security Efforts, *Information Week*, March 29, 26.
18. Hunter, Richard & Mogull, Rich (2003) Role of Government in Protecting Cyber-Infrastructure, *Gartner Research Note*, October 21, 1.

19. Irvine, C., Chin, S-K. & Frincke, D. (1998) Integrating Security into the Curriculum, *Computer*, 31 (12), December, 25–30.
20. Kahan, Steve (2004) Information Security: On the Cusp of a Management Evolution, in *Management of Information Security*, Whitman, Michael E. & Mattord, Herbert J. (Course Technology: Boston, Massachusetts), 18-19.
21. Kelly, C. J. (2005) Enough I Quit, *Computerworld*, January 10, 30.
22. Kim, Y., Shim, S.J. & Yoon, K.P. (1999) Bridging the Gap between Practitioner-Educator Perceptions of Key Information Systems Issues for Effective Implementation of Information Systems Curriculum, Proceedings of the 1999 IRMA International Conference, Hershey, Pennsylvania, May, 513-518.
23. King, Julia (2004) Grooming Next Generation Information Technology Professionals, *Computerworld*, August 23, 32.
24. Kirkpatrick, Terry A. (2002) Re-Thinking Risk, *CIO Insight*, September, 65-66.
25. Lee, Denis M.S., Trauth, E. & Farwell, D. (1999) Critical Skills and Knowledge Requirements of Information Systems Professionals: A Joint Academic / Industry Investigation, *MIS Quarterly*, 19, September, 313-340.
26. Lightfoot, J.M. (1999) Fads Versus Fundamentals: The Dilemma for Information Systems Curriculum Design, *Journal of Education for Business*, 75 (1), September / October, 43-50.
27. Lindquist, Christopher (2004) Security Super-Group, *CIO Magazine*, January 15, 94.
28. Maglitta, J. (1996) Information Systems Schools: Need Improvement, *Computerworld*, February 19, 78-83.
29. McCreary, Lew (2004) Are We Converged Yet?, *CSO Magazine*, December, 8.
30. Miller, K.W. (1997) Computer Security & Human Values Interact, Proceedings of the ASEE / IEEE Frontiers in Education Conference, IEEE, 1025-1029.
31. Mullin, Ted R. (2004) Information Technology Employment Outlook, Presentation, Information Systems Education Conference, Newport, Rhode Island, November 13, 3.
32. National Security Agency (2004), <http://www.nsa.gov>, Centers of Academic Excellence – Criteria for Measurement, Centers of Academic Excellence – Institutions, Committee on National Security Systems (CNSS) – CNSS Library Files, Information Assurance (IA) Courseware Evaluation Program – Overview and History, National Information Assurance Education & Training Program - Standards, December.
33. Petersen, Scot (2004) Wanted: Cyber-Security, *eWeek*, October 18, 38.
34. Ragatz, Gary L. (2004) Thinking About Business Education, *Decision Line*, Decision Sciences Institute, 35 (4), July, 12.
35. Roberto, Michael A. & Carioggia, Gina M. (2002) Launching the War on Terrorism, *Harvard Business Review*, October 17, 11.
36. Roosevelt, Margot (2005) Homeland Security 101, *Time*, January – December, 20.
37. Sarkar, Dibya (2004) The End of the Beginning: Homeland Security Technology Enters a New Era, *Federal Computer Week*, December 8, 3.
38. Spaford, E. (1998) Teaching the Big Picture of INFOSEC, Proceedings of the National Colloquium for Information Systems Security Education, Arlington, Virginia, 1.
39. Squire, Jonathan (2003) Leading Barriers, *Computerworld*, July 21, 53.
40. Srinivasan, S. Guan, J. & Wright, A.L. (1999) A New Computer Information Systems Curriculum Design Approach for the 21st Century, *Journal of Computer Information Systems*, 39, (3), 99-106.
41. Stahl, Stephanie (2004) Information Technology Training, Certification and e-Learning, *Information Week*, March 29, 88.
42. Thibodeau, Patrick (2004) Information Technology Security Boom, *2004 Information Security Global Workforce Study*, November, 1.
43. Thurrott, Stephanie (2004) Cyber-Sleuths, *Information Technology Link*, 3 (1), Winter, 16.
44. U.S News & World Report (2004) http://www.usnews.com/usnews/edu/college/directory/alpha_dir/brief/index_brief.php, October.
45. Verton, Dan (2004) Information Technology Hurdles Complicate Intelligence Overhaul, *Computerworld*, August 23, 6.
46. Verton, Dan (2002) Experts Predict Major Cyber-Attack Coming. *Computerworld*, July 8, 8.
47. Vijayan, Jaikumar (2004) Security Professionals Bemoan Need for Tactical Focus, *Computerworld*, November 15, 4.

48. Webster, William H. (1998) Cyber-Crime, Cyber-Terrorism and Cyber-Warfare: Averting an Electronic Waterloo, *Global Organized Crime Project of the Center for Strategic & International Studies*, xiii,2.
49. Weinberger, Joshua (2004) Special Report: Security, *CIO Insight*, March, 85.
50. Whitman, Michael E. & Mattord, Herbert J. (2004) *Management of Information Security*. (Course Technology: Boston, Massachusetts), 186.

NOTES