

2004

# The Education of Information Security Professionals: An Analysis of Industry Needs vs Academic Curriculum in the 21st Century

Albert L. Fundaburk

*Nova Southeastern University*, [afundaburk@outlook.com](mailto:afundaburk@outlook.com)

This document is a product of extensive research conducted at the Nova Southeastern University [College of Engineering and Computing](#). For more information on research and degree programs at the NSU College of Engineering and Computing, please click [here](#).

Follow this and additional works at: [http://nsuworks.nova.edu/gscis\\_etd](http://nsuworks.nova.edu/gscis_etd)

 Part of the [Computer Sciences Commons](#)

## Share Feedback About This Item

---

### NSUWorks Citation

Albert L. Fundaburk. 2004. *The Education of Information Security Professionals: An Analysis of Industry Needs vs Academic Curriculum in the 21st Century*. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, Graduate School of Computer and Information Sciences. (531)  
[http://nsuworks.nova.edu/gscis\\_etd/531](http://nsuworks.nova.edu/gscis_etd/531).

This Dissertation is brought to you by the College of Engineering and Computing at NSUWorks. It has been accepted for inclusion in CEC Theses and Dissertations by an authorized administrator of NSUWorks. For more information, please contact [nsuworks@nova.edu](mailto:nsuworks@nova.edu).

The Education of Information Security Professionals: An Analysis of Industry Needs vs.  
Academic Curriculum in the 21<sup>st</sup> Century

by

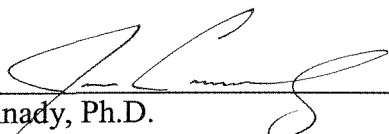
Albert L. Fundaburk

A dissertation submitted in partial fulfillment of the requirements for the degree of  
Doctor of Philosophy

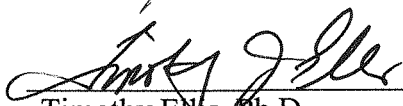
Graduate School of Computer and Information Sciences  
Nova Southeastern University

2004


We hereby certify that this dissertation, submitted by Albert L. Fundaburk, conforms to the acceptable standards and is fully adequate in scope and quality to fulfill the dissertation requirements for the degree of Doctor of Philosophy.

  
\_\_\_\_\_  
James Cannady, Ph.D.  
Chairperson of Dissertation Committee

7/11/04  
Date

  
\_\_\_\_\_  
Timothy Ems, Ph.D.  
Dissertation Committee Member

7/11/04  
Date

  
\_\_\_\_\_  
Michael Laszlo, Ph.D.  
Dissertation Committee Member

7/11/04  
Date

Approved

  
\_\_\_\_\_

Edward Lieblein, Ph.D.  
Dean, Graduate School of Computer and Information Sciences

7-11-04  
Date

Graduate School of Computer and Information Sciences  
Nova Southeastern University

An Abstract of a Dissertation Submitted to Nova Southeastern University in Partial  
Fulfillment of the Requirements for the Degree of Doctor of Philosophy

The Education of Information Security Professionals: An Analysis of Industry Needs vs.  
Academic Curriculum in the 21<sup>st</sup> Century

by

Albert L. Fundaburk

June 2004

This research compared the employment of the skills and attributes needed by information systems security professionals in an information systems security work environment with those taught in NSA Centers of Academic Excellence in Information Assurance Education. Using two surveys the goal of this research was to determine if the skills and attributes identified in the CISSP were employed in an information systems work environment and if these skills were taught in colleges and universities designated as NSA Centers of Academic Excellence in Information Assurance Education.

The skills and attributes within the 10 domains of the CISSP were identified by 23 questions contained in two surveys, one to information systems security professionals working in the field and one to information systems security faculty in NSA designated Centers of Academic Excellence in Information Assurance Education. The CISSP domains cover the following areas of information security responsibilities: 1) *Access Control Systems and Methodology*, 2) *Telecommunications and Network Security*, 3) *Security Management Practices*, 4) *Applications and Systems Development Security*, 5) *Cryptography*, 6) *Security Architecture and Models*, 7) *Operations Security*, 8) *Business Continuity Planning and Disaster Recovery Planning*, 9) *Laws, Investigations, and Ethics*, and 10) *Physical Security*. The CISSP domains were chosen as the defining criteria for the development of the operational definitions after an extensive review of literature in the field of information security.

The surveys were developed over three phases: the pilot phase, the validity phase, and the reliability phase. The breakdown of the domain descriptions into questions was accomplished during the pilot survey phase.

Requests for participation in the survey were e-mailed to 800 information systems security professionals and 321 information systems security faculty. There was a 67% information systems security faculty response rate and a 20% information systems security professional response rate.

This research indicated that information systems security professionals working in an information systems security work environment employed or addressed the skills and attributes identified in the 10 domains of the CISSP. This research also indicated that the skills and attributes taught in the curriculum of NSA Centers of Academic Excellence in Information Assurance Education had no association with the skills and attributes employed, or addressed, by information systems security professionals in an information systems security work environment. There was one exception, Domain 4, *Applications and Systems Development Security*, which indicated there was an association between how the skills and attributes were employed in an information systems security work environment and were taught in NSA Centers of Academic Excellence in Information Assurance Education.

The findings of this research can be used as a baseline to develop information systems security curriculum. Further research is needed to determine the differences, if any, in the skills and attributes identified in the various information security certifications, the correlation between the skills and attributes identified in each of the information security certifications, and any differences in the employment of these skills and attributes between certified and non-certified information systems security professionals.

## Acknowledgements

Many people have provided support and assistance during the research and writing of this dissertation. Several of them deserve special thanks.

The successful completion of this work would not have been possible without the invaluable guidance of my dissertation committee in shaping and refining this research: Dr. James Cannady, my committee chair, for his support, timely advice and especially for his encouragement when it was needed most; Dr. Timothy Ellis for his methodology expertise, without which I would have floundered; and Dr. Michael Laszlo for his technical expertise.

My colleagues in the CIS and OIS Departments at Bloomsburg University of Pennsylvania provided invaluable assistance by serving on the pilot and validity panels. Special thanks go to the faculty members in the Business Education/Office Information Systems Department for picking up many of my additional duties and allowing me to concentrate on completing this research.

My most heartfelt thanks and love go to my wife, Karen. She persevered throughout the entire progression. She read, reread, and offered comments on each and every draft. Her support and encouragement during the many frustrations inherent in this process enabled me to continue. I can truly say it would not have been completed without her.

# Table of Contents

**Abstract**   iii  
**List of Tables**   ix

## **Chapters**

### **1. Introduction**   1

Problem Statement and Goal   1  
Relevance and Significance   4  
Barriers and Issues   6  
Research Questions   6  
Limitations and Delimitations   7  
Definition of Terms   8  
Summary   17

### **2. Review of Literature**   19

Introduction   19  
Historical Overview   21  
Information Technology   23  
Information Systems Security   29  
Certification   41  
Curriculum Design   43  
Information Systems Security Curriculum   49  
Summary   62

### **3. Methodology**   64

Research Methods   65  
  Procedures Used to Develop the Survey   66  
  Develop the Conceptual Framework   66  
  Develop the Operational Definitions   67  
  Select the Scaling Technique   67  
  Review of Items   68  
  Develop Response Format   71  
  Develop Directions   72  
  Prepare Draft and Distribute Pilot   72

Analyze Pilot Study and Revise Instrument (if required)	73
Produce Instrument	73
Conduct Validity and Reliability Analysis	74
Distribute Surveys	79
Discussion	80
Formats for Presenting Results	82
Resource Requirements	83
Summary	83

#### **4. Results 85**

Statistical Tools Used in Analysis	85
Statistical Analysis and Findings	87
Domain 1 Analysis	87
Domain 1 Findings	93
Domain 2 Analysis	94
Domain 2 Findings	96
Domain 3 Analysis	97
Domain 3 Findings	102
Domain 4 Analysis	103
Domain 4 Findings	106
Domain 5 Analysis	107
Domain 5 Findings	111
Domain 6 Analysis	111
Domain 6 Findings	116
Domain 7 Analysis	117
Domain 7 Findings	120
Domain 8 Analysis	121
Domain 8 Findings	124
Domain 9 Analysis	125
Domain 9 Findings	129
Domain 10 Analysis	131
Domain 10 Findings	132

#### **5. Conclusions, Implications, Recommendations, and Summary 134**

Conclusions	134
Implications	139
Recommendations	140
Summary	141

#### **Appendixes**

<b>A. Pilot Survey Committee Members</b>	<b>146</b>
<b>B. Pilot Survey Cover Letter</b>	<b>147</b>
<b>C. Pilot Survey</b>	<b>149</b>



<b>D. Pilot Survey Evaluation Procedures</b>	<b>153</b>
<b>E. Pilot Survey Comments and Responses</b>	<b>155</b>
<b>F. Face Validity Committee Members</b>	<b>156</b>
<b>G. Validity E-mail Round One</b>	<b>157</b>
<b>H. Validity Survey Round One</b>	<b>159</b>
<b>I. Validity Results Round One</b>	<b>169</b>
<b>J. Validity E-mail Round Two</b>	<b>174</b>
<b>K. Validity Survey Round Two</b>	<b>175</b>
<b>L. Validity Results Round Two</b>	<b>176</b>
<b>M. IRB Approvals</b>	<b>177</b>
<b>N. Survey E-Mails</b>	<b>180</b>
<b>O. Information Systems Security Faculty Survey</b>	<b>187</b>
<b>P. Information Systems Security Professional Survey</b>	<b>191</b>
<b>Q. SPSS Statistical Results</b>	<b>195</b>
<b>R. Raw Data</b>	<b>225</b>
<b>References</b>	<b>233</b>

## List of Tables

### Tables

1. Qualifications of Content Validity Panel 74
2. Split-halves Results for Reliability Phase 78
3. Cronbach's Alpha Reliability Analysis 78
4. Frequency Table for Edu6 102
5. Frequency Table for Edu10 107
6. Frequency Table for Pro10 107
7. Frequency Table for Pro20 130
8. Frequency Table for Edu20 130

## Chapter 1

### Introduction

#### **Problem Statement and Goal**

In recent years, there has been a dramatic shift in the way computers are used. The advances in computer security have not kept pace with the phenomenal advances in computers and networking. Due to these advances the need is continuous for trained security professionals. To address this need the National Security Agency (NSA) established the Centers of Academic Excellence in Information Assurance Education program.

Recent high-profile computer attacks, like those against the Web sites of Yahoo and Amazon.com, while not necessarily typical, raised security concerns at companies and universities. With the Internet established as a fact of life for businesses, and networked computers increasingly indispensable to our daily lives, people who know how to protect computers are a hot commodity. Unfortunately, academic programs that teach such expertise are lagging far behind this demand (McCollum, 2000, p. 38).

The Internet has allowed a world so interconnected that work cannot be accomplished without computers, and computers cannot perform effectively without a measure of security. Due to the shortage of information systems security professionals a need exists for a comprehensive program to educate more individuals in the field of Information security (Chin & Frincke, 1997). Employers expect graduates to have the proper technical

and non-technical skills to ensure success. The rapidly evolving information systems environment requires up-to-date education.

Although professional certifications in information security are based on a common body of knowledge, there is still a fundamental difference of opinion as to what constitutes a common body of knowledge. Many practitioners of information security feel that to further define information security and to legitimize its existence there should be accredited college curricula (Saita, 2002). Information security as a field has not matured sufficiently to develop processes associated with performing specific information security job tasks. Until these tasks are identified and related job standards produced, effective standardized information security curricula can not be developed (Reynolds, 1998).

The National Security Agency's Centers of Academic Excellence in Information Assurance Education identified 37 universities as meeting the standards required for recognition as Centers of Academic Excellence in Information Assurance Education. One of the standards for compliance stipulated that schools must have curriculum mapped to National Security Telecommunications and Information Security Committee (NSTISSC) *4011 National Training Standard for Information Systems Security (INFOSEC) Professionals*, an eight year old document (Centers of Academic Excellence in Information Assurance Education, 2002). The NSTISSC focus was to provide standards for practical vocational skills. Mainstream colleges and universities have goals that may or may not be compatible with those of the standards dictated by NSTISSC (Yasinsac, 1999). The Security Certification Consortium (ISC)<sup>2</sup> was instrumental in the development of the Certified Information Systems Security Professional (CISSP), the

most comprehensive certification for information systems security professionals (Dugan & Prencipe, 2001). A comparison of the NSTISSC required standards and the CISSP domains indicated there was no standard for *Access Control Systems and Methodology*, Domain 1 of the CISSP, in the NSA document, and other domains were covered haphazardly. Although CISSP was not the only certification available for information systems security professionals, it was the only broad top-down certification covering theoretical knowledge of 10 domains recognized to be required for information security certification and for many organizations the CISSP was considered to be the gold standard in information security (Dugan & Prencipe, 2001). It was this theoretical requirement that needed to be the baseline for identifying skills and attributes for a common body of knowledge in information security, which determined whether academia was providing education in this common body of knowledge.

This research examined the 10 CISSP domains from within the information systems security work environment to determine which skills were deemed necessary and then examined existing NSA Centers of Academic Excellence in Information Assurance Education curriculum to determine which skills and attributes from within the 10 domains were being taught. An on-line survey was developed to identify the skills and attributes of an effective information systems security professional using the 10 domains of the CISSP examination. Using empirical methods the goal of this research was to determine if existing curriculum in colleges and universities designated as NSA Centers of Academic Excellence in Information Assurance Education was consistent with the needs of an information systems security work environment.

## Relevance and Significance

Kim and Choi (2002) stated that the determination of key educational requirements for information systems security professionals by experts in the field was important in the development of an information systems security curriculum. Golshani, Panchanathan, Friesen, Park, & Song (2001) observed that a formal definition of the basic principles of information security did not exist and that this lack contributed to an unstructured approach to information security.

As of 2002, information systems curriculum was driven by the National Security Agency's Centers of Academic Excellence in Information Assurance Education. The award of this designation was dependent upon meeting 10 specific criteria for measurement.

The number one criteria for designation mandated that the academic program of the university be tied to NSTISSI 4011, with courses mapped to NSTISSI 4012, 4013, 4014, and 4015. The other criteria included:

- 1) the academic program must be multidisciplinary
- 2) the university must have information security plans and programs in place
- 3) the university must encourage research in information security
- 4) the university must share knowledge
- 5) the faculty must be active in research
- 6) the library must contain up-to-date reference materials
- 7) the program must have declared programs of certification or tracks
- 8) there must be a declared center for information security maintained by the university

- 9) the faculty must be obtained across departmental lines (Centers of Academic Excellence in Information Assurance Education, 2002).

*The National Training Standard for Information Systems (INFOSEC) Professionals, NSTISSI 4011*, (1994), consisted of seven areas: a) Communications Basics, b) Automated Information Systems Basics, c) Security Basics, d) NSTISS Basics, e) Systems Operating Environment, f) NSTISS Planning and Management, and g) NSTISS Policies and Procedures. Although this document was information security specific the material was dated and did not cover information security as it related to current issues. A comparison of NSTISSI 4011 and the CISSP domains identified areas not covered (CISSP Certification Common Body of Knowledge Study Guide, 2000). Individual courses must be mapped to *NSTISSI 4012, National Training Standard for Designated Approving Authority*, *NSTISSI 4013, National Training Standard for Systems Administrators in Information Systems Security*, *NSTISSI 4014, National Training Standard for Information Systems Security Officers*, and *NSTISSI 4015 National Training Standard for Systems Certifiers*. In a report of the 1998 annual meeting of the National Colloquium for Information Systems Security Education, Reynolds (1998) stated that information security education must avoid the parochial mind-set of using what is best for government as a baseline for the information security profession.

A search of existing literature supported the need for a standard curriculum in information security. Bishop (2000), in particular, identified this need in two specific articles. In his presentation to the National Colloquium on Information Systems Security he defined information security as it applied to academia and stated the goal of undergraduate, graduate, and doctorate education was to “learn

broad principles, and see how to apply them” (Bishop, 2000). In a presentation to the National Colloquium on Information Security Education, he outlined the following shortcoming of existing curriculum. At the undergraduate level curriculum is more focused on application of principles as opposed to the critical analysis of those principles. This tends to provide graduates with a distorted view of computer security. Students who want a deeper understanding of these principles are relegated to independent study or graduate courses. Graduate courses tend to focus on the design and specification of secure systems but rarely implement the designs. Computer security should apply both to be successful (Bishop, 1997).

### **Barriers and Issues**

The analysis of information security presented a number of significant problems.

These included:

- 1) addressing the interdisciplinary nature of information, and
- 2) defining the depth and scope of knowledge which will satisfy the designation of a security professional.

This research performed a rigorous review of information security skills and attributes in preparation for determining the depth and scope of knowledge required.

### **Research Questions**

This research provided answers to the following questions:

- 1) Are the skills and attributes identified in the CISSP used in an information systems security work environment?



- 2) Are universities designated as National Security Agency Centers of Academic Excellence in Information Assurance Education providing these skills?

### **Limitations and Delimitations**

The following limitations to the research were noted:

- 1) Only participants who held a CISSP certification and worked in an information systems security environment participated in the information systems security professional survey.
- 2) Only participants who have taught or were teaching an information security course in an NSA designated Centers of Academic Excellence in Information Assurance Education institution participated in the information systems security faculty survey.

The following delimitations to the research were noted:

- 1) Only security professionals on the CISSP Web list, February 2003, participated in this research.
- 2) Only faculty from universities designated as NSA Centers of Academic Excellence in Information Assurance Education as of February 2003, participated in this research.

The following assumptions to the research were noted:

- 1) The 10 domains of the CISSP fairly define skills and attributes needed in an information systems security environment.
- 2) Academic institutions designated as NSA Centers of Academic Excellence in Information Assurance Education are familiar with the 10 domains of the CISSP.

## **Definition of Terms**

According to Krutz and Vines, (2001) the following definitions apply to information security:

### Access control

The process of limiting access to the resources of a particular system to authorized users, programs processes or other systems.

### Access control matrix

A table in which each row represents a subject, each column represents an object and each entry is a set of access rights for that subject to that object.

### Access control mechanism

Hardware or software features, operating procedures, management procedures, and combinations that are designed to detect and prevent unauthorized access and to permit authorized access to a particular system.

### Access level

The hierarchical portion of the security level that identifies the sensitivity of the data and the clearance of authorized users.

### Accountability

The property that enables activities on a system to be traced to individuals who may be held accountable for their actions.

### Assurance

The degree of confidence that security needs are satisfied.

## Authenticate

To verify the identity of a user, device, or other entity as a prerequisite for entry into a protected system or to verify the integrity of data that has been stored, transmitted, or otherwise exposed to unauthorized modification.

## Authenticator

The means used to confirm the identity or to verify the eligibility of a station, originator, or individual.

## Bell-La Padula model

A formal state transition model of computer security policy that describes a set of access control rules.

## Biometrics

An automated means of identifying or authenticating the identity of a living person based on physiological or behavioral characteristics.

## Certification

The comprehensive evaluation of the technical and non-technical security features of an information system that establishes the extent to which the system meets a specified set of security requirements.

## Clark-Wilson commercial security policy

The policy established to maintain consistency between the internal data and user expectations.

### Computer cryptography

The use of a crypto-algorithm in a computer, microprocessor, or microcomputer to perform encryption or decryption in order to protect information, or to authenticate users, sources, or information.

### Contingency management

Establishing actions to be taken before, during, and after a threatening incident.

### Contingency plan

A plan for emergency response, backup operations and post-disaster recovery maintained as part of a security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

### Countermeasures

Any action, device, procedure, technique, or other measure that reduces the vulnerability or threat to a system.

### Crypto security

The security or protection resulting from the proper use of technically sound crypto systems.

### Crypto-algorithm

A well-defined procedure or sequence of rules used to produce a key stream or cipher text from plain text or vice-versa.

## Cryptography

The principles, means, and methods for rendering information unintelligible and for restoring encrypted information to readable form.

## Data integrity

The property that data meet an expected level of quality.

## Data security

The protection of data from any unauthorized modification, destruction, or disclosure.

## Denial of service

Any action that prevents any part of a system from functioning in accordance with its intended purpose.

## Disaster

A sudden unplanned, catastrophic event that brings about damage or severely diminishes an organization's ability to provide critical business functions for some undetermined period of time.

## Disaster recovery plan

Written procedures for emergency response, extended backup operations, and post-disaster recovery after a loss of computer resources and/or physical facilities.

## Domain

The unique context in which a program is operating or a set of objects that a user has the ability to access.

### File protection

The aggregate of all processes and procedures in a system designed to inhibit unauthorized access, contamination, or elimination of a file.

### Formal security policy model

A mathematically precise statement of a security policy that represents the initial state of a system, the way a system progresses from one state to another, and the definition of a secure state of the system.

### Graham-Denning model

This model operates on eight primitive protection rights that can be issued by subjects, with effects felt on other objects or subjects.

### Handshake

A dialog between two entities for the purpose of identification and authentication.

### Individual accountability

The ability to positively associate a user with the time, method, and degree of access to a system.

### Information flow control

A procedure to ensure information transfers within a system are not made from a higher security level to a lower security level.

### Least privilege

The principle that requires each object to be granted the most restrictive set of privileges needed to perform authorized tasks.

### Mandatory access control

A means of restricting access to objects based on the sensitivity of the object and the clearance of the subject desiring access.

### Modes of operation

A description of the conditions under which an information system functions based on the sensitivity of the data and the authorizations of the user.

### Object

A passive entity that contains or receives information.

### Password

A protected/private character string that is used to authenticate an identity.

### Penetration

The successful act of bypassing the security mechanisms of a system.

### Permissions

A description of the type of authorized interactions a subject can have with an object.

### Physical security

The application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and sensitive information.

## Protocols

Protocols are a set of rules and formats, semantic and syntactic, which permit entities to exchange information.

## Recovery planning

The advance planning and preparations that are necessary to minimize loss and to ensure the availability of the critical information systems of an organization.

## Recovery procedures

The actions necessary to restore computer capability and data files to a system after a systems failure.

## Reliability

The probability of a system performing its mission adequately for a specified period of time under expected environments and operating procedures.

## Risk

The probability that a particular threat will exploit a particular vulnerability of a system.

## Risk analysis

The process of identifying security risks, determining their potential, and identifying areas in need of safeguarding.

## Risk management

The total process of identifying, controlling, and eliminating or minimizing uncertain events that might affect system resources.



### Security measures

Elements of software, firmware, hardware, or procedures in a system to satisfy security specifications.

### Security policy

The set of laws, rules, regulations, and practices that regulate how an organization manages, protects, and distributes sensitive information.

### Security policy model

A formal presentation that identifies the set of rules and practices that regulate how an organization manages, protects, and distributes sensitive information.

### Spoofing

An attempt to gain access to a system by posing as an authorized user.

### State variable

A variable that represents either the state of the system or the state of some system resource.

### System integrity

The quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

### Tampering

An unauthorized modification that alters the proper functioning of a system in a manner that degrades its security or functionality.

### Technical attack

An attack perpetrated by circumventing or nullifying hardware and software protection mechanisms.

### Technical vulnerability

A hardware, firmware, communication, or software flaw that leaves a system vulnerable to attack.

### Threat

Any circumstance or event that has the potential to cause harm to a system.

### Threat analysis

The examination of all actions and events that might cause harm to a system or operation.

### Threat monitoring

The analysis, assessment, and review of audit trails and other data that are collected for the purpose of searching for systems events that might constitute violations or attempted violations of system security.

### Trusted computer system

A system that employs sufficient hardware and software assurance measures to enable its use for simultaneous processing of a range of sensitive or classified information.

### Un-trusted process

A process that has not been evaluated or examined for adherence to security policy.

### User

A person or process accessing an information system either by direct or indirect connections.

### User ID

A unique symbol or character string that is used by a system to identify a specific user.

### User profile

Patterns of user activity that can be used to detect changes in normal operations.

### Vulnerability

A weakness in system security procedures, systems design, implementation, or internal controls that could be exploited to violate systems security.

### Vulnerability assessment

A measure of vulnerability that includes the susceptibility of a particular system to a specific attack.

## **Summary**

The rapidly evolving information systems environment requires up-to-date information security curriculum. The speed in which the information systems environment changes in regard to security makes it extremely difficult for a university

curriculum to prepare students for working in the world of information security. The problem was that current schools and universities recognized as Centers of Academic Excellence in Information Assurance Education were mapping curriculum to an eight year old document.

This research provided answers to the following questions:

- 1) Are the skills and attributes identified in the CISSP used in an information systems security work environment?
- 2) Are universities designated as National Security Agency Centers of Academic Excellence in Information Assurance Education providing these skills?

To answer these questions, this research examined the 10 CISSP domains from within the information systems security work environment to determine which skills were deemed necessary and then examined existing NSA Centers of Academic Excellence in Information Assurance Education curriculum to determine which skills and attributes from within the 10 domains were being taught. With the 10 domains of the CISSP as a baseline an on-line survey was developed to identify the skills and attributes of an effective information systems security professional. Using empirical methods the goal of this research was to determine if existing curriculum in colleges and universities designated as NSA Centers of Academic Excellence in Information Assurance Education was consistent with the needs of an information systems security work environment.

## Chapter 2

### Review of Literature

#### **Introduction**

The review of literature examined several aspects of information systems and information security. The introduction and historical overview explores information technology and its relationship to organizations. The second section defines information technology. The third section investigates information systems security. The fourth section identifies specific certifications in information security. The fifth section explores curriculum design in information technology. The sixth section explores specific curriculum development in information systems security.

Several steps were used for the purpose of reviewing existing literature and research. Initially, the following databases were used: ACM Digital Library, Applied Science and Technology, Computer Abstracts, Computer and Information Systems Abstracts, ProQuest, and EBSCOhost. The searches were conducted by focusing on keywords used in each of the databases. The keywords used were: information technology (IT), infosec, information security, information security education, computer security, computer security curriculum, information systems curriculum, CISSP, information systems security certification and information systems security requirements. The second step required reviewing all documents, journals, texts, and books,

identified using these keywords, for applicability to the research. In all cases the listed references in these documents, journals, texts and books were analyzed and those meeting the criterion were requested from the library at Bloomsburg University and again reviewed for applicability to the research.

The third step required reviewing the documents pertaining to the research and rating them using the following categories: relevance, date of article, and type of publication (refereed, non-refereed, commercial, or in-house).

The review of literature revealed limited research on the actual tasks required for success as an information systems security professional. Although numerous articles discussed information security curriculum, very few were empirical in nature, nor rigorous in the research used in developing the curriculum.

As early as the 1990s there were predications showing an increased demand for information security. To this end the National Colloquium for Information Systems Security Education (NCISSE) set forth the following goals in 1998:

- 1) to bring together industry, government, and academia to define current and emerging requirements for security education
- 2) to discuss future direction of information security education at the graduate and undergraduate level
- 3) to form an advisory group to act as a forum for continued communications
- 4) to encourage colleges and universities to teach information systems security courses in various curricula to meet the needs of 21<sup>st</sup> century consumers
- 5) to increase course offerings to meet the growing demand for information systems security professionals (Reynolds, 1998, p.1)

The NCISSE is not an implementing body, but does offer suggestions to industry, government, and academia. The suggestions offered in 1998 included:

- 1) Develop standards for what information systems security professionals should know and be able to do

- 2) 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.
- 3) Develop credentials for skills
- 4) Develop standards or metrics for IT infrastructure security with heavy reliance on those for other more established infrastructures
- 5) Identify the role of “best practices” in the profession and address the question “whose best practice”
- 6) Overcome resistance among information security to the standards of rigor and discipline that are expected of other professions (Reynolds, 1998, p.2)

Davis and Dark (2002) presented a report to NCISSE addressing information assurance curriculum development. This report detailed the participants, processes, and procedures of two curriculum workshops held in 2001. These workshop participants included stakeholders from government, industry, and academe. The workshops used the input of these stakeholders to determine the curriculum outline for both graduate and undergraduate education. Although the workshops produced a creditable document, the data collection was neither rigorous nor empirical. The following suggestion as outlined by the 1998 NCISSE, “Develop standards for what information systems security professionals should know and be able to do” (Reynolds, 1998) has yet to be fulfilled.

### **Historical Overview**

Although research, primarily federally funded, was common in the 1970s, its emphasis was on confidentiality, especially in the government which dominated security technology.

Building on the 1960s and 1970s efforts to model information flows and protect schemes in computer systems, the National Security Agency (NSA) developed the Trusted Computer System Evaluation Criteria, known formally as the Orange Book, and the Trusted Product Evaluation program. In the 1980s the NSA established an outreach organization, the National Computer Center, to promote the Orange Book. Activities associated with the Orange Book were intended to foster broader development, acquisition and use of more secure computing

systems by addressing the problem of limited information and understanding through dissemination of criteria for security product development and product certification. The criteria had limited impact because of their narrow technical assumptions, bureaucratic conduct associated with product evaluation and certification, the application of export controls to associate products and mismatch with the commercial marketplace (Blumenthal, 1999, p.525).

During the 1980s the growing use of databases led to an increased scrutiny in integrity. *The Computer Security Act of 1987* provided a foundation for information security with an emphasis on privacy and security plus sensitivity to the needs of both civilian and military perspectives. It was in the 1990s, with the widespread use of networked information systems, that the focus led to availability. The federal government recognized the impact of information security on the national infrastructure in July of 1990 by implementing the *National Policy for the Security of National Security Telecommunications and Information Systems*. This directive established the initial policies and organizational structure to guide the conduct of activities to secure the national information infrastructure (NSTISSI, 1990).

The growth of information systems technology and the corresponding threats have been further recognized by the government. In July of 1996, Executive Order 13,010 established the President's Commission on Critical Infrastructure Protection to assess and respond to threats across interdependent infrastructures: telecommunications and information services, electric power, oil and gas distribution, transportation, water, banking and finance, emergency services, and government services (Blumenthal, 1999). However, in a report of the 1998 annual meeting of the National Colloquium for Information Systems Security Education, Reynolds (1998) cautioned against using what is best for government as a baseline for the information security profession. In October of 2001, Executive Order 13,231 renamed the National Security Telecommunications and



Information Systems Security Committee, established by *National Policy for the Security of National Security Telecommunications and Information Systems*, as the Committee on National Security Systems. The subcommittee established to deal explicitly with information security was the Subcommittee on Information Systems Security with the overall responsibilities to:

- 1) develop, formulate, and recommend operating policies, objectives and priorities required to achieve broad information systems security
- 2) maintain an understanding of the security initiatives that are undertaken with the private sector in accordance with national policy
- 3) provide a forum for the exchange of security guidelines
- 4) oversee the development of the annual assessment on the security status of national security systems
- 5) develop information systems security guidance
- 6) interact with various subcommittees on implementation of appropriate security protective measures
- 7) provide reports and identify actions and topics that require the attention of the committee (National Security Agency, 2001).

The areas most pertinent to the objectives and goals as identified by this literature search included:

- 1) Information Technology
- 2) Information Systems Security
- 3) Certification
- 4) Curriculum Design
- 5) Information Systems Security Curriculum

### **Information Technology**

To understand the role of information security on the existing and future network infrastructure it is necessary to understand the impact of information technology on the organization.

Torkzadeh and Doll's (1999) empirical research on the impact of technology on work supported the research findings that the success of information technology can potentially be measured through its impact on work at the level of the individual end-user.

Organizations were concerned about how the millions spent on information technology influenced organizational and individual performance and were looking for a means of validating this expense. The explicit objective of Torkzadeh and Doll's (1999) research was to develop an instrument that:

- 1) identifies the multidimensional nature of information technology's impact at the level of the individual end-user
- 2) is short, easy to use and appropriate for both academic research and practice
- 3) can be used with confidence across a variety of applications and contexts (p.328).

Torkzadeh and Doll's (1999) research reported on an initial effort to conceptualize the extent of the impact for the following dimensions of information technology:

- 1) Task productivity: the extent that an application improves the user's output per unit of time.
- 2) Task innovation: the extent that an application helps users create and try out new ideas in their work.
- 3) Customer satisfaction: the extent that an application helps the user create value for the firm's internal or external customers.
- 4) Management control: the extent that an application helps to regulate work processes and performance (p.329).

Based on an extensive literature review the researchers generated 39 items to measure the aspects of this impact. The pilot study involved generating a structured interview questionnaire and process to assess the validity of the instrument. The responses to the questionnaire were reviewed with these objectives in mind: purification, unidimensionality, reliability, brevity, and simplicity. Eighty-nine usable interviews were obtained using this pilot study process. The initial 39 question survey was reduced to a

four factor, 12 item instrument and verified the four dimensions of information technology's impact on work. This four factor, 12 item instrument was distributed to 409 end-users across a wide spectrum of industries and the results analyzed to further validate the instrument's reliability.

The final analysis of the survey indicated that the survey did have adequate reliability and validity. Torkzadeh and Doll (1999) recommended further research to confirm the measurement model, evaluate the stability of the instrument, and develop standards for evaluating specific applications.

Organizations were increasingly confronted with changing strategic issues brought about by deregulation, globalization, ubiquitous connectivity, and the convergence of industries and technologies. The ability of an organization to respond to these issues depends on having sophisticated and technical infrastructure. There was a gap, in even the most competitive organizations, between emerging strategic direction and information technology's ability to support it. Working with more than 500 senior executives, Prahalad and Krishnan's (2002) research identified the nature and seriousness of this disconnection. These senior executives, when asked about their capacity to lead change in their organizations, identified the quality of the information technology infrastructure as an impediment to this effort. The most common constraints centered on legacy infrastructure, incompatible databases and applications, poor quality of data, restricted scalability, and business processes trapped in vendor software modules. A lag in information infrastructure often stymied key dimensions of strategic needs.

Attempts to create business models enabled by technology have shown mixed results. Companies with a high degree of technology acumen failed because they underestimated

the complexities of logistics, while companies with an understanding of logistics failed in their ability to attract customers, and link suppliers and partners using technology (Prahalad & Krishnan, 2002).

Among the many causes of this disconnect between managerial imperatives and information infrastructure capabilities were the changes in business environment and technology, management's approach to information technology, and the role information technology played in the strategic process. Over the last decade the changes in technology that significantly affected the organization included:

- 1) the public network infrastructure
- 2) operating systems
- 3) database management
- 4) business applications (Prahalad & Krishnan, 2002, p.26).

With the exception of business applications there seemed to be a convergence in many of these technology changes. The key to acceptable change in business applications was to design the system to take into consideration the cost of change and the time to implement. In many instances business application changes were implemented with a standard user interface and no regard for future needs. To improve efficiency many organizations adopted large enterprise applications predestined by the vendor. This required vendor participation when change was implemented. Over the last five years, companies have invested over \$300 billion in these enterprise systems, with less than adequate return. These solutions were seen as a quick fix to the legacy inspired problems (Prahalad & Krishnan, 2002).

Prahalad and Krishnan's (2002) research identified three questions that senior business managers need to ask before implementing information technology investments:

- 1) Does the application architecture and underlying infrastructure in the enterprise reflect the company's strategic vision?
- 2) What are the inherent risks and impediments to change embedded in our information infrastructure?
- 3) What does a viable portfolio of IT capabilities look like (p.27)?

It also identified a common framework for understanding the capabilities, impediments, and risks associated with the information technology application infrastructure:

- 1) What is the role of application in strategy?
- 2) Is knowledge about the business process domain stable or evolving?
- 3) How much does the application get changed?
- 4) Where do we source the application?
- 5) What is the nature of the data?
- 6) What are the quality problems (p.29)?

For each application system in the infrastructure the need remained to determine whether the business processes encompassed in that application are core to organizational strategy.

Increasingly, information technology managers struggle with conflicting strategic imperatives of innovation, efficiency and flexibility. However, without the active understanding of the technical and organizational impediments to tying IT to the organization's strategic tasks, the disconnection between efficiency and flexibility cannot be bridged (Prahalad & Krishnan, 2002).

The evolution of society from industrial based to knowledge based has increased the importance of IT and IT professionals in providing organizational information. The challenges of managing IT in this environment will continue to increase in complexity. It is impossible to define an effective business strategy that does not rely on IT:

Today, information technology is ubiquitous. It is integral to processes internal to the firm, product design, delivery of services, and inter-organizational relations. It

is the lifeblood of the organization, shrinking the effects of time and distance and altering the very nature of work (Benamati, 1999, p.144).

Although very little research has directly addressed the problems of IT change and how management copes with it, broadly related issues have been considered. Research has also investigated organizational issues caused by a changing environment. The purpose of Benamati's (1999) research was to test the theory that changing dimensions of the environment cause management problems for IT organizations.

Benamati (1999) used a field survey to determine the extent to which subject organizations had experienced 39 specific problems on recent major development, implementation, and support efforts underway during three prior years. The questions used a scale of 1 – 7 where 1 meant "to no extent" and 7 meant "to a very great extent". A pilot study was conducted with five IT professionals to validate the survey, which was to ensure the survey was clear, concise, and that the items portrayed their intended meanings. The results were incorporated in the final instrument. There was some question as to the instrument validity process as five IT professionals to validate 39 questions may not be sufficient. The survey instrument was mailed to a random population of 1,000 IT professionals. The first mailing identified 874 non-respondents. A second mailing resulted in a usable sample of 246 responses.

The analysis proceeded in two stages. The first employed confirmatory factor analysis (CFA) to examine the problem and coping mechanisms categories proposed in the revision of the environmental impact theory. The second stage used the results of the first to test the hypothesis about the relationship between problems and coping mechanisms (Benamati, 1999).

Model generation is the most common used application of CFA. In this approach, an initial model was tested for fit against collected data. If fit was not adequate the model was adjusted and re-tested. Benamati (1999) used three determiners of statistical fit:

1. A chi square ratio
2. Bentler and Bonnet's non-formed fit index
3. Bentler's comparative fit index.

The final result of the study found nine of the preliminary problem types supported in the research, while two were not.

As IT is considered a strategic resource and given to changing at a rapid rate the management of IT has increased in importance. Benamati's (1999) research identified problems that occur due to this change and the coping mechanisms being applied to these problems. It also discussed the relationships between IT problems and coping mechanisms. The recognition of changes brought about by the risk of internetworking, and identifying the coping mechanisms dealing with these changes, is extremely important to any research on the implementation of information security.

### **Information Systems Security**

The importance of information systems security was confirmed by the 2002 CSI/FBI Computer Crime and Security Survey. This survey clearly showed a marked increase in computer security incidents and a significant rise in financial losses. It identified an increase in total annual losses attributed to computer security incidence from \$100 million in 1997 to \$456 million in 2002. Over the past five years the total losses have exceeded \$1 billion. In 2002, 91% of the respondents detected security breaches compared to 90% detected in 1999. Comparisons of the surveys from 1996 through 2002

show a significant increase in the Internet as a frequent point of attack (POA) (The International Information Security Foundation (I<sup>2</sup>SF) , 2002). The IT Risk Management Series (1999), compiled by Ernst & Young, found 66% of the respondents not using the Internet would begin to utilize it, and 83% respondents using the Internet would increase usage, if security concerns were adequately addressed.

The Department of Defense (DoD) established new information security architecture entitled *Technical Framework for Information Management (TAFIM)*. It was the defining document in *Department of Defense Goal Security Architecture (DGSA)*. However, it has not been implemented, although a number of events have been identified as required for future implementation. Feustel and Mayfield (1998) have provided numerous challenges as to how DGSA concepts can be implemented efficiently, including exploring the implications of some of the wider range of security issues brought about by implementation.

In 1993 the DoD identified a new set of requirements which would lead to a major alteration in DoD's approach to information security. The requirements stated that DoD must:

- 1) Support information processing under multiple security policies of any complexity or type, including those for sensitive unclassified information and multiple categories of classified information.
- 2) Be sufficiently protected to allow distributed information processing (including distributed information systems management) among multiple hosts on multiple networks in accordance with open systems architecture.
- 3) Support information processing among users with different security attributes employing resources with varying degrees of security protection, including users of non-secure resources if a particular mission so dictates.
- 4) Be sufficiently protected to allow connectivity via common carrier (public) communications systems (Feustel & Mayfield, 1998, p.4).



Further supporting these requirements, the Chairman of the Joint Chiefs of Staff issued the following policy with respect to Defensive Information Operations:

- 1) Information, information-based processes, and information systems (such as command, control, communications, and computer (C4) systems, weapons systems, and infrastructure systems) used by the US military forces will be protected relative to the value of the information contained therein and the risks associated with the compromise of or loss of access to the information.
- 2) Information systems defense relies on four interrelated processes. These include a process to protect information and information systems, a process to detect attacks or intrusions, a restoration process to mitigate the effects of incidents and restore services, and a response process (Feustel & Mayfield, 1998, p.4).

One significant change in DoD policy was its movement away from a dedicated infrastructure to public switched networks. The establishment of these requirements indicated that DoD had a clear understanding of information security protection from both a government and commercial standpoint. This switch required that accessibility alone be provided by the public network with all other security requirements placed at the endpoints of the network. DoD's organizational structure has much in common with the commercial sector. It has payroll, human resources, invoicing, purchasing, and accounting. However, DoD has many unique policy elements such as the protection of classified information (Feustel & Mayfield, 1998). This type of access control was regulated on a need to know basis. While access control was specifically focused on the management of information sharing, such controlled sharing was difficult at best in a shared-resource environment. Feustel and Mayfield (1998) identified four options to manage shared-resource access:

Current sharing options include: 1) uncontrolled sharing wherein systems operate in an unprotected mode, 2) discretionary sharing in which information owners can designate under their own authority who may share access to the owned information, 3) "systems high" sharing in which all data and programs can be

treated as having sensitivity of the most classified information and programs on the system and all users must be cleared to this sensitivity level, and 4) the uniform application of system wide, non-discretionary access controls, often referred to as mandatory access control ( p.6).

DoD's mandatory access control systems were difficult to implement and were often of little interest to commercial operators.

DoD recognized the cost effectiveness of using off-the-shelf software as in requirement three above. The challenge was to implement the system in such a way that security policy implementation and enforcement were:

- 1) relatively transparent to the user's program
- 2) highly intuitive when the user abides by the security policy
- 3) only obvious when the user does not abide by the policy (Feustel & Mayfield, 1998, p.7).

Feustel and Mayfield (1998) maintained that implementation of policies emphasizing access control and prevention of information flow seem simple compared to assuring that the security policies are executed properly and that the change in DoD requirements indicate a change in philosophy within the government regarding information management.

Information security should protect confidentiality, integrity, and availability of information systems. With the widespread use of the Internet and understanding the nature of this use as being information intensive, information security was a growing spending priority among most companies. Gordon and Loeb (2002) introduced a model which took into account the vulnerability of the information to a security breach, as well as the risks and return on investment of these risks. The results of this analytical research suggested that to maximize the expected benefit from investment to protect information a company should only spend a fraction of the expected loss.

The importance of information security is noted by the large amount of research, most of which was focused on the technical aspects. Gordon and Loeb's (2002) article sought to derive an economic model that determined the optimal amount to invest in information security. This model specifically considered how the vulnerability affected the optimal amount of resources that should be devoted to securing that information.

Gordon and Loeb's (2002) research considered a one-period model of a firm contemplating the provision of additional security to protect given information sets. The increased security could be with respect to confidentiality, integrity, and availability. Gordon defined an information set as characterized by the loss conditioned on a breach occurring, the probability of a threat occurring, and the probability that a threat, once realized, would be successful.

Some of the outcomes supported by Gordon and Loeb (2002) included:

- 1) For a given potential of loss, a firm can be better off concentrating its resources on high-vulnerability information sets.
- 2) A firm should be careful in deciding where to concentrate information security resources.
- 3) The optimal investment in information security is always less than or equal to 36.79% of the loss that would be expected in the absence of any investment in security (p.453).

Gordon and Loeb's (2002) analysis showed that:

For a broad class of security breach probability functions, the optimal amount to spend on information security is an increasing function of the level of vulnerability of such information. Our analysis also shows that for a second broad class of security breach probability functions the optimal amount to spend on information security does not always increase with the level of vulnerability of such information (p.453).

Future empirical research should assess whether organizations actually invest in information security consistent with the outcomes of this article.

To successfully defend against security breaches organizations developed security policies. The practicality of an information policy depended on whether that policy was enforceable and at what cost. Some class enforcement mechanisms work by monitoring execution steps of some system and terminate the execution if it is about to violate the security policy being enforced.

For the most part these general purpose applications-dependent security policies have attracted the most attention. However, special purpose security policies are increasingly important (Schneider, 2000). The importance of application-dependent and special purpose policies, defined as execution monitoring (EM), was explained using the Principle of Least Privilege which states that each principle is given the minimum access needed to accomplish the task. The practicality of this, or any, security policy is dependent upon enforceability and cost.

Schneider (2000) defined the above application-dependent security policies as follows:

- 1) Access control defines safety properties. The set of proscribed partial executions contains those partial executions ending with an unacceptable operation being attempted.
- 2) Information flow does not define sets that are properties, so it does not define sets that are safety properties. Not being safety properties, there are no EM enforcement mechanisms for exactly this property.
- 3) Availability, if taken to mean that no principle is forever denied use of some given resource, is not a security policy (p.35).

However, Schneider (2000) noted availability that rules out all denials in excess of some predefined maximum wait time was considered a security policy and real systems security policies were best written in modules, or a collection of simpler policies.

Schneider (2000) further noted that large single entity policies were difficult to

implement and comprehend. Beyond comprehension there were other advantages to collections of small policies:

- 1) Having a collection allows different enforcement mechanisms to be used for different automata (hence the different security policies) in the collection.
- 2) Security policies specified by distinct automata can be enforced by distinct system components (p.46).

Some significant benefits accrue from having the source of all of an automaton's input symbols as a single component. These include:

- 1) Enforcement of a component's security policy involves trusting only that component.
- 2) The overhead of an enforcement mechanism is lower because communication between components can be reduced (Schneider, 2000, p.42).

Schneider (2000) believed a precise characterization was given for the class of security policies enforceable with mechanisms that work by monitoring system execution, and automata were introduced for specifying exactly that class of security policy.

Another major information security concern involved e-commerce. Many organizations were using e-commerce to tap a far-reaching global market. Inexpensive access and the graphical interface of the Internet provided tremendous opportunities for companies to expand using e-commerce to conduct business across their customer base. However, there were impediments to the success of this expansion. Rose (1999) identified six commonly recognized categories of technological impediments to e-commerce: 1) download delays, 2) limitations of the interface, 3) search problems, 4) inadequate measurement of Web application success, 5) security (or perceived security) weaknesses, and 6) lack of Internet standards. Although the six recognized impediments

to e-commerce were important, the security weakness impediments were most relevant to this research.

Although the customer has established an Internet connection to the retailer and the transmission of data is within bounds, threats to e-commerce still exist. The most common of these threats is security. This threat exists for both the customer and the retailer. According to Rose (1999) there was sufficient technology to secure the data from the client to the server. However, there appeared to be serious security issues in preventing hackers from attacking the client and server themselves.

Transaction security was primarily concerned with either privacy or the guarantee that sender and receiver are who they are supposed to be. The infrastructure of the Internet was such that messages were being passed in a shared domain. Anyone with access to that domain could view all the messages being sent. Under these conditions it was best to assume that unauthorized users were viewing these messages (Rose, 1999). Although the encryption or authentication technology existed to combat this, many companies were slow to use this technology. Thus, a primary weakness in Internet security was the failure to use either encryption or authentication. Encrypted messages, when used correctly, were better protected from all but the most dedicated criminal interceptor. Using these technologies secured the transaction process to the point that the biggest dangers to security occurred after the data was transferred to the retailer's server (Rose, 1999).

Conducting e-commerce created the potential of greater access to the corporate databases. However, security threats to the retailer's server and access by disgruntled employees existed whether or not the organization conducted e-business. While

sophisticated firewalls and other security measures existed, many hackers appeared to be one step ahead of available security (Rose, 1999).

These perceived threats were seen by customers as real, so that customers were not yet comfortable with sending personal information across the Internet. In spite of existing technologies it was estimated that 6 million Americans have been victims of e-commerce fraud or related credit card misuse. He maintained that in spite of the existing security technologies, Internet security was a serious threat to business-to-consumer e-commerce and that transactional security was a managerial rather than a technical problem (Rose, 1999).

Intrusion detection systems were in their infancy. Within discussion of network intrusions or penetrations it was not always clear as to what constituted misuse, or which types of misuse could be construed as illegal. Rosenthal (1999) defined computer misuse as "the performance of an action that is not desired by the system owner, one that does not conform to the system's acceptable use and/or security policy". Regardless of the determination of criminology, the number and complexity of computer and network attacks were growing at an alarming rate with very little being done to effectively prevent them. However, the damage caused by this misuse can be contained with the implementation of an Intrusion Detection System (IDS). IDS has become more sophisticated since its introduction, and in the years 1997 and 1998, the market for IDS grew from \$40 million to \$100 million, primarily due to the steady increase in computer breaches. The use of IDS cannot be implemented in a haphazard manner and be expected to be effective. The implementation requires careful planning, phased deployments, and specialized training (Rosenthal, 1999). According to the National Institute of Standards

and Technology (NIST) there are three viable ways to justify the costs of implementing IDS. These are:

- 1) The first way rests on the fact that intrusion-detection technology can detect attacks that cannot be prevented. Sophisticated hackers with experience and know-how can penetrate most networks because of the existence of network vulnerabilities that cannot be fixed (e.g. legacy computers with operating systems that are no longer updated or patched). Even current and updatable systems are often neglected because of inexperienced administrators or the absence of a viable policy or procedure to ensure that available system updates and patches are applied correctly and in a timely manner.
- 2) The second way an organization can justify an IDS is obvious; intrusion-detection technology can prevent attackers from probing the network. A network that does not have operational intrusion-detection resources is an open invitation for attackers to probe for existing weaknesses without fear of retribution, knowing that vulnerabilities will eventually be found and possibly exploited.
- 3) And finally, intrusion-detection systems can provide proof of attack and can characterize and verify both internal and external threats. This leads to intrusion accountability, and it provides a third way to justify their existence (Rosenthal, 1999, p.37).

To be effective there must have been a comprehensive review of existing security policies and procedures, and thought must have been given to how IDS will fit into the overall security plan and the security goals of the organization. At a minimum the security goals should have included:

- 1) Confidentiality: only authorized users can read or copy a given file or object.
- 2) Control: only authorized users can decide when to allow access to information.
- 3) Integrity: only authorized users can alter or delete a given file or object.
- 4) Authenticity: correctness of attribution or description.
- 5) Availability: no unauthorized users can deny authorized users timely access to files and other system resources.
- 6) Utility: fitness for a specified purpose (Rosenthal, 1999, p.37).

The open systems architecture of the Internet created an environment in which hackers and attackers exploited security vulnerabilities locally or from a distance, although



research indicated that more than three quarters of all misuse activities originate from within an organization (Rosenthal, 1999).

Rosenthal (1999) defined network or systems intrusions as “any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource” and broke down these intrusions into two main categories:

- 1) Misuse intrusions, which are well planned or orchestrated attacks that target a system’s weak points, but can be detected by watching for certain actions being executed on certain objects or systems.
- 2) Anomaly intrusions, which are deviations from established normal system usage patterns that can be detected by creating a “normal use” profile of the system being monitored and comparing deviations from that profile (p.38).

Computer intrusions were classified with respect to six different and distinct motives:

- 1) Government and military: attempting to access information of national strategic importance.
- 2) Business: attempting to gain a competitive advantage by obtaining design or source code information.
- 3) Financial: attempting to obtain direct financial gain by stealing credit card information or stealing/transferring money from bank accounts.
- 4) Terrorist: attempting to cause damage by attacks on computers rather than by way of traditional methods.
- 5) Grudge: personal retaliation resulting in the destruction of computing resources.
- 6) Fun: attempting to gain access for enjoyment rather than personal gain or profit (Rosenthal, 1999, p.38).

Rosenthal (1999) described the protocols that encompass most attacks, which he stated were usually in this order:

- 1) Reconnaissance: information gathering.
- 2) Probe and attack: identify weaknesses and deploy attack tools.
- 3) Toehold: exploits known weaknesses and secures entry to the system.
- 4) Advancement: migrate from an unprivileged to a privileged account.
- 5) Stealth: install “backdoor” tools, and covers an attacker’s tracks.
- 6) Listening post: establish a listening or monitoring posture.
- 7) Takeover: expand intruder control from single host to multiple hosts or networks (p.38).

These sophisticated attack scenarios and innovative penetration methods required extremely complex detection mechanisms to which IDS systems had not yet evolved. Although IDS technology was seen by many as a “cure all” many IDS products were still in the development stage. Intrusion detection was not without its pitfalls and problems, and these continued to detract from the effectiveness and dependability of the intrusion detection process (Rosenthal, 1999).

Information security was not the only aspect of security needing definition. The American Society for Industrial Security convened the Fourth Annual Academic/Practitioner Symposium to create an undergraduate and graduate program in industrial security in which the chair, stated “There are no clearly illuminated paths to good security education” (Longmore-Etheridge, 2000). Prior to the symposium a pre-survey was used to identify content for future security courses and information systems security emerged as a major player:

The topics from the survey results were: physical security, personal security, information systems security, investigations, loss prevention, risk management, legal issues, emergency planning, fire protection, crisis management, disaster management, counterterrorism, competitive intelligence, executive protection, and violence in the workplace, crime prevention, crime prevention through environmental design, and security architecture and engineering (Longmore-Etheridge, 2000, p.63).

Symposium participants were divided into groups to create graduate and undergraduate courses. The graduate group identified the core areas that they would like to see in security curriculum. These core areas included:

- 1) Legal and Investigative Aspects of Risk Management
- 2) Information Security, and Information Systems Threats and Security and Security Concepts and Organizational Leadership
- 3) Design of Integrated Systems
- 4) Business Functions of Security
- 5) Special Issues and Current Trends

6) Methodology (Longmore-Etheridge, 2000, p.63).

The undergraduate group finalized the core areas to include:

- 1) Business and Organizational Security Risk Management
- 2) Physical Security Systems; Integration and Analysis
- 3) Personnel and Information Security System
- 4) Security Management in the Business Environment (Longmore-Etheridge, 2000, p.64).

In addition to developing a core of courses for undergraduate and graduate education, the security industry tried to develop a security body-of-knowledge. This body of knowledge defined who security professionals were, what security stood for, and its diversity of topics. This body-of-knowledge used the following model to define requirements:

- 1) Determine Objectives
- 2) Design Protection Systems
- 3) Evaluate the Protection Systems

By using this structure, roles and responsibilities were defined so others can recognize the value security adds to the organization (Longmore-Etheridge, 2000).

### **Certification**

The CISSP was a broad top-down certification (Dugan & Prencipe, 2001) created by the International Information Systems Security Certification Consortium (ISC)<sup>2</sup> which was supported by the Computer Security Institute, Information Systems Security Association, the Canadian Information Processing Society, as well as other industry presences (Sumner & Werner, 1997). (ISC)<sup>2</sup> was instrumental in the development of the CISSP, which was considered the most comprehensive certification for information systems security professionals.

A new certification was developed by the (ISC)<sup>2</sup> in 2002 which addressed the need for certification as a practitioner in systems security. It also encompassed seven domains of information security, some of which were similar to the CISSP domains. This certification stressed the need for a practitioner of information security whereas CISSP outlined a more general and deeper knowledge of information security. Both were recognized as definitive certifications in the field of information security and were essential to the development of the domains used by this research in identifying tasks performed in an information systems security environment. For many organizations the CISSP was considered to be the gold standard in information security (Dugan & Prencipe, 2001).

The study guide for the CISSP Common Body of Knowledge (CBK) domains was considered the key to obtaining the CISSP certification. This study guide outlined CBK requirements for certification as an Information Systems Security Professional. Krutz and Vines (2001) have written extensively on mastering the 10 domains listed in the CISSP CBKs. Their *CISSP Preparatory Guide* is one of the few books with detailed knowledge of the requirements needed to become a CISSP certified security professional.

Other certifying bodies include the International Information Security Foundation which formed a committee to develop and promulgate generally accepted security principles. The outcome of this committee was the document known as the Generally Accepted Systems Security Principles (GASSP). This document was produced in 1992.

Rather than another ad hoc effort, the GASSP decided to establish an Authoritative Foundation of existing works that, through their broad acceptance, have articulated, in one way or another, the GASSP of the information security profession. Recognizing the hierarchic nature of principles, it was determined to use the Organization for Economic Cooperation and Development (OECD) Information Security Principles, with their international acceptance, as the

model for the foundation of the GASSP hierarchy, the Pervasive Principles, and, through a careful analysis and mapping of the Authoritative Foundation and derivative works, to develop Broad Functional Principles, as accepted and supported by consensus of the IT industry and profession. Finally the GASSP will develop Detailed Principles, including "how to" guidance.

The development of a consensus-building process is central to the success of this approach. Other key tasks include the establishment of linkages to the Common Criteria and the (ISC)<sup>2</sup> sponsored CISSP designation.

Finally, two essential elements, which will be evolutionary in nature, are to be developed. The first is the definition and establishment of an authoritative infrastructure, or governing body. This effort has been initiated. Second is the development of models for legislative/regulatory initiatives that have the support of the profession, industry, and government. Their purpose will be to establish the "glue" that effectively binds the consolidation of these complex issues internationally.

#### OBJECTIVES:

- 1) The international harmonization of culturally neutral information security
- 2) The elimination of artificial barriers to the free flow of information worldwide
- 3) The definition and implementation of a principled foundation for an industry, the success of which is critical to the future of the Information Age and its ramifications for privacy and security
- 4) Provision for the rapidly evolving nature of information security methods, issues, and technology, and their articulation in principle
- 5) Recognition and correlation to related management issues. (The International Information Security Foundation (I<sup>2</sup>SF), 1991, p.3).

The CISSP was based in part on the GASSP results (Grimaila & Kim, 2002).

#### Curriculum Design

The 21st century will see significant changes in information technology. E-commerce, broadband technology for the home, home based networking, and video conferencing are representative of these changes. The IT professional will be tasked to keep up with these changes through continuous education and training. Lightfoot (1999) observed that educational institutions should shoulder the burden for the preparation of

information technology professionals for the vibrant environment of the upcoming century.

It is the responsibility of the education system, particularly at the college undergraduate level, to prepare future information technology professionals for the dynamic environment of the 21<sup>st</sup> century. This preparation has a dual purpose. First, it must give students the necessary skills in current industry practices to satisfy requirements for an entry level position. Second, it must provide students with the fundamental background and abilities to learn new skills throughout their career. In effect, teaching current skills helps student secure their first job, whereas teaching fundamentals helps them get subsequent jobs (p.43).

Lightfoot (1999) identified problems that institutions face due to the speed of change in information technology. He cited research which indicated that technology courses emphasizing fundamentals were being scaled back in favor of other less technical offerings.

Basically, the problem is one of balance between the dual purposes of a college level education. The temptation is to overemphasize the current trendy topics at the expense of more mundane, fundamentals-based curriculum (p.43).

However, businesses had a very pragmatic view of information technology curriculum. They would prefer that colleges and universities generate a steady stream of graduates with expertise in tools and applications so that entry level students were productive upon hiring (Lightfoot, 1999).

Lightfoot (1999) identified three basic categories of curriculum design and discussed the pros and cons of each:

A large amount of excellent research has been performed to determine the proper curriculum design for an undergraduate college level IS program. The research of this type can generally be grouped into three categories:

1. Proposed model curricula generated by professional organizations
2. Surveys to determine the specific skills that academics or professionals think an IS student should have for the future
3. Case studies of curriculum in a specific IS department (p.50).

This research was most concerned with category two “Surveys to determine the specific skills that academics or professionals think an IS student should have for the future”. Lightfoot (1999) identified specific problems he felt were associated with this method of curriculum development. Lightfoot (1999) stipulated that it did not take into consideration the time lag needed to actually produce graduates. Depending on the institution it can take anywhere from one to three years to implement a new program, with between five to eight years before a student graduates with the new skill set.

According to Lightfoot (1999) the major problem with future-oriented IS curriculum survey research was that:

It forces the department to use a short-term perspective to implement long-term planning. It is doomed to fail in most cases and places IS curriculum designers in a position of constantly chasing a moving target. The conclusions from the literature concerning new, emerging skills and obsolete, sundown skills make this point. There will always be new skills on the horizon that businesses want. The curriculum design process should not be regulated to “chasing rainbows” to satisfy business (p.59).

In IT curriculum development academic institutions must consider how organizations implement IT training. Foreign competition, increased efficiency, and the speed of technological advances have forced businesses to take a close look at the role end-users and end-user training play in the organization. In the age of knowledge workers, white collar college-educated employees were the future users of information technology. The prime objective of end-user technology training was to help the organization achieve its goals through the optimum use of its personnel. As technology expanded, the knowledge required to use this technology expanded and training became more important. Desai and Von Der Embse (2001) stated that due to this expansion of technology, end-user

computer skills become obsolete in a short period of time. Effective training can reduce, if not eliminate, the difference between actual and desired end-user performance.

End-user computing required not only a firm background in information technology, but an understanding of various organizational functions:

Thus, a student who aspires to be an information systems manager must have both the business knowledge and the technical ability to apply the tools used in business. If an MIS curriculum is totally based on IT, it might produce an acceptable IT expert. However, this expert is not sufficiently versed on its implications for business process and functions (Desai & Von Der Embse, 2001, p.553).

Information technology education and its interrelationship with businesses were key variables in the success of information technology curriculum. Information technology in this instance referred to any technology that, directly or indirectly, made information available to the end-user in any organization or in society. This included information security. Whenever this new technology was introduced to an organization its members were required to retrain their skills to maintain their performance level. As a result most organizations have used one or more of the following approaches to accomplish this retraining:

- 1) Self-training or On the Job Training (OJT) – refers to the training an employee gets while at work. This type of end-user training can be obtained via manuals, a mentor/tutor, or distance learning, intranet, or by trial and error.
- 2) In-house training – denotes formal training an individual's employer provides via scheduled instruction on their organizational premises. Organizations such as Texas Instruments and EDS have in-house training programs for their end-users of IT.
- 3) Outside training- many organizations outsource some part of formal training to outside training consultants. The outside training may be due to unavailability of or greater cost of in-house expertise for a specific technology.
- 4) Formal education – in some cases, employees may be required to pursue a formal degree program (Desai & Von Der Embse, 2001, p.555).



In light of the above approaches, many universities began to revisit their strategy for developing information technology curriculum and began to provide specific training to their students such as preparation for specific certifications. To be successful institutions were required to differentiate information technology education from specific information technology training. An integrated approach was needed incorporating specific training, conceptual education, and business management education. In educational institutions this integration required a partnership between information technology educators, business educators, and business managers. Information technology faculty should have assessed industry trends for specific future information technology requirements.

This synergistic approach to information technology curriculum development will be very useful to future graduates in an information technology program. This approach also validated the requirements for the development of a baseline common body of knowledge for information security.

Bishop (2000) began his keynote speech to the National Colloquium on Information Systems Security with the following statement:

The last four years have seen an explosion in the concern for the security of information. People are becoming aware of how much information is publicly available, as stories in the national news media discuss the ease with which identities are stolen. On a less personal note, compromises of information involving people authorized to access that information show that both companies and governments have problems in securing information. With this awareness has grown an understanding of our dependence on accurate, confidential information as well as the fragility of the infrastructure we use to secure that information. Of all the questions emerging, the fundamental one is; how can we secure information (p.1)?

In this speech Bishop (2000) defined the current practice in information security education as meeting the National Plan for Information Systems Protection. However, this plan has yet to define information security education in any meaningful way. He stipulated that:

The report makes cursory mention of the interdependence of the various forms of education, and focuses primarily on training, awareness, and providing support for government and industry, and for academic programs that support the efforts of the government's plan directly (p.1).

The document clearly underscored that the education being discussed was training, although support for undergraduate work was provided through Scholarship for Service.

This speech further defined the goals and advantages of good undergraduate education. Bishop (2000) stipulated that the goal of undergraduate education was to learn broad principles and apply them. The advantage of obtaining this goal was the breadth of learning obtained. There was an emerging interest in improving the state of information systems security education. The desired improvements included establishing core curricula and integrating computer security into more aspects of information technology education. NSA was on the forefront of this drive with its Centers of Academic Excellence in Information Assurance Education Program:

Specifically, the Centers of Academic Excellence in Information Assurance Education has as one evaluation criterion that the academic program demonstrates information security is not treated as a separate discipline, but as a multidisciplinary science with the body of information assurance knowledge incorporated into various disciplines (Bishop, 2000, p.8).

NSA stipulated the goals of this program were to create a climate of independent research in information assurance.

Bishop (2000) outlined the goals of information security education and discussed the progress being made in meeting these goals:

- 1) We are making minimal progress in integrating information security into other parts of our curricula.
- 2) We have not learned from our mistakes, and continue to repeat errors from the past.
- 3) We have not improved how we design systems and programs to account for security constraints, nor have we reduced the number of security patches necessary.
- 4) We are learning how to abstract the requisite characteristics of a system towards this end, but we have much to learn.
- 5) We do not understand how humans interact with systems, how security problems arise from this interaction, and therefore cannot use this knowledge to build systems that minimize the possibility and effects of errors (p.10).

His final statement in this speech supported the need for a comprehensive and definitive baseline in the skills needed for information security curricula:

All forms of education, from basic research to training are critical to responding effectively to the information security crisis we face now. In addition to focusing our efforts on training, we should focus our efforts on basic research and higher education. The latter two will provide the teachers and researchers to train systems administrators, business executives, and management in the intricacies of information security that affect them and their organizations. Further, the emphasis on basic research will lead to more research faculty in the area of information security, thereby seeding more universities and academic institutions with people who can teach and do research in that area (Bishop, 2000, p.11).

### **Information Systems Security Curriculum**

Dr. Cynthia Irvine, on faculty at the Naval Post Graduate School (NPS), was instrumental in developing the information security curriculum at NPS and has written extensively on its implementation. The school designed the program as a track within its computer science curriculum. This track conveyed vital concepts in current information security concepts (Irvine, Warren, & Clark, 1997). Irvine's article, *Goals for Computer Education*, identified two different approaches to computer security education. One approach was to treat security as an ad hoc set of functions. The second approach was to build security into systems using an engineering-oriented approach based on fundamental

principles (Irvine, 1996). One significant issue faced by information security curriculum developers using an engineering-oriented approach was whether to stress basic fundamentals or current applications that tend to be vendor specific. Lightfoot (1999) suggested that a combination of the two should be included in any curriculum development process. In his keynote speech to the National Colloquium on Information Systems Security Education Bishop (1997) identified the problems with current information systems security and outlined the future direction of information systems security education needed to ensure success in an information systems security environment. He stated the past curriculum was concerned with the application of principles and operational issues whereas the emphasis has been on the analysis of the principles themselves.

Carnegie Mellon University supported the contention that there is no set of skills identified as being necessary in information security curriculum development:

There apparently is no systematic agreement on the knowledge, skills, and abilities required to formulate a curriculum for information assurance and security professionals that enjoys a broad-based support across organizations (“Information Assurance Curriculum”, 1999).

There was pressure from the government to provide some minimum level of competence for systems and network professionals working in the field of information assurance. One initiative that attempted to address this problem was NSA’s development of the National INFOSEC Education and Training Program which established the Information Assurance Courseware Evaluation Process. This process was intended to assess the degree to which various institutions, colleges, and university curricula satisfied the NSTISSI standards.

Many professional organizations began to recognize the importance of information security for their membership by offering certifications in information security.

The International Federation of Information Processing (IFIP) has issued a statement on information security assessment and certification as part of an effort to establish international certification standards for individuals accessing information technology systems and the information security management of those systems. IFIP held the First World Conference on Information Security Education in Stockholm in June 1999.

The Information Systems Audit and Control Association (ISACA) provides the Certified Information Systems Auditor Program. The American Society of Industrial Security (ASIS) provides certification for general security management. USENIX Systems Administrator's Guild (SAGE) has a certification subcommittee currently studying certification for systems administrators ("Information Assurance Curriculum", 1999).

Other organizations worked with accreditation institutions to ensure a viable information security curriculum.

The Association for Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE) have relationships established with organizations that are involved with accreditation of higher-education computer science and engineering programs. However, accreditation does not get to the level of granularity that includes requirements for information security curricula ("Information Assurance Curriculum", 1999).

Many other professional organizations offer courses and conferences to their members as part of a continuing education process. For example, Information Systems Security Association (ISSA) provides continuing technical education forums and conferences.

More and more universities are offering graduate and undergraduate programs in information security. In 1999 there were fewer than six universities conforming to NSA's criteria for becoming a Center of Academic Excellence in Information Assurance Education. In 2002 there were 37 universities meeting the criteria required by the NSA ("Centers of Academic Excellence", 2002).

The business community recognized the need for information security. However, a majority of information security training in the private sector was vendor specific.

Some vendors, such as Cisco Systems, have curriculum tracks that cluster technology specializations and provide certification designations, such as “Cisco Certified Network Professional” with a specialization in security (“Information Assurance Curriculum”, 1999).

Bishop (2000), in his report to the National Colloquium on Information System Security stated that to rely on vendor specific education would not provide a well rounded information systems security professional.

The NSA developed a program to recognize colleges and universities with information assurance programs meeting published criteria based on training standards established by the NSTISSC. The overall curriculum has to be mapped to *NSTISSI 4011 National Training Standards for Information Systems Security (INFOSEC) Professionals*. As this document was developed in June of 1994, a comparison of the CISSP domains and this standard revealed serious gaps in the requirements as dictated by the NSA (“Centers of Academic Excellence”, 2002). NSA is afflicted with an image problem due, in part, to its mandate to be able to break into, as well as protect systems. These conflicts have been epitomized in controversies relating to its cryptographic policy (Blumenthal, 1999).

Golshani, F., Panchanathan, S., Friesen, O., Park, Y., and Song, J. (2001) observed that a formal definition of the basic principles of information security did not exist and that this lack contributed to an unstructured approach to information security. Yang (2001) discussed the need of higher education to become involved in training both university students and on-the-job professionals. His analysis of what should be taught was based on an analysis of existing certification requirements of the following major agencies:

- 1) Certified Information Systems Auditor
- 2) Certified Information Systems Security Professional
- 3) System and Network Assurance Program
- 4) Systems Administration, Networking, and Security.

As of 2002, information systems curriculum was driven by the NSA's Centers of Academic Excellence in Information Assurance Education. The award of this designation was dependent upon meeting 10 specific criteria for measurement. In a review of the curriculum for the 37 universities designated as Centers of Academic Excellence in Information Assurance Education, Logan (2002) found that undergraduate education was not a popular option for curriculum in information security.

Recognizing the connection between information security and emerging information technologies, John Hopkins University created the Information Security Institute which conducted research, offered classes and degree programs, created business relationships, and held open forums in broad topics centered on information security (Piazza, 2001). The chairman of John Hopkins University's Computer Science Department described the new program as interdisciplinary:

We see the development of new types of hybrid degrees taking a holistic approach to the information security area, in recognition that it's not only a technical field but deals with issues in policy, standards, law, ethics, and many other areas. Customized degrees might include a cross between an MBA and a computer science degree. In addition, the institute will address a range of issues from critical infrastructure protection to national and international economics to intellectual property protection. Many other degree combinations are possible among these disciplines (p.40).

Recognition by the NSA as a Center of Academic Excellence in Information Assurance Education required individual courses be mapped to *NSTISSI 4012, National Training Standard for Designated Approving Authority, NSTISSI 4013 National Training*

*Standard for Systems Administrators in Information Systems Security, NSTISSI 4014*  
*National Training Standard for Information Systems Security Officers, and NSTISSI 4015*  
*National Training Standard for Systems Certifiers.* In 1997 the term “assurance” was propagated because of its ambiguity for most people and its meaning to information systems security professionals (Blumenthal, 1999).

Protection of information assets had been a major challenge from the beginning of the computer age. Given the widespread use of information technology for day-to-day business operations, and the continued use of the Internet to conduct business, the need to protect our business infrastructure was critical. University graduates who are information security literate and are equipped with the proper knowledge can alleviate many of the issues regarding information security. The task of integrating information security into existing computer science programs is complicated. Yang (2001) suggested that information security curriculum designers address the following questions prior to developing their curriculum:

- 1) How would we prepare our students so they would be security literate?
- 2) Given the fast advancement of computer technology, how would a faculty member become security aware and capable of teaching the new tools and techniques?
- 3) In addition to technical solutions of computer security (such as firewalls, encryption, access controls, audit trails, training, benchmarking, interoperability, et al), should and how would the curriculum cover non-technical aspects such as social, cultural, political, legal, economic, and organizational issues?
- 4) Should computer security be integrated throughout the curriculum, or should special courses and/or tracks be created to address the needs?
- 5) Should alternative curriculum delivery mechanisms be used? Examples include Web based delivery, continuing education courses, corporate training, distance education, et al (p.236).

He has also identified seven basics of computer security education:

- 1) Understand and comply with security policy and laws



- 2) Recognize potential security problems in their environment
- 3) Know how to be proactive in preventing security problems
- 4) React appropriately to an occurrence of a security problem
- 5) Know where to find additional help or information
- 6) Make informed decisions on security matters
- 7) Speak the language (p.239).

Yang (2001) made seven specific observations regarding the development of an information security curriculum:

Observation #1: Involvement of higher education in computer security is urgently needed in training both college students and on-the-job professionals, in order to meet the challenges of protecting the information infrastructure.

Observation #2: It is important to address the ethical and cultural issues in the computer security curriculum.

Observation #3: A majority of computer security curriculum involves extension of traditional Computer Science curriculum, such as networking, programming, databases, et al.

Observation #4: Computer security education is more than just providing training on technical topics. It should contain components that address business and managerial aspects of computer security, such as law, investigations, ethics, physical security, and business continuity and disaster recovery.

Observation #5: Similar to other computer professions, the abilities of the students to recognize and analyze a problem and get a “handle” on it is critical for being successful in the profession of computer security.

Observation #6: Similar to integrating any new major technology into the Computer Science education, the integration of computer security into the undergraduate programs requires strong support from the Administration.

Observation #7: The process of integrating computer security into a program is a continuous process and involves the faculty’s involvement in multiple activities, including research, professional development, curricular design, and teaching (p.240).

The integration of computer security into existing computer science was complicated; however, it was urgently required. Yang’s (2001) observation #4, in particular, supported the need for the development of a common body of knowledge in information security which contained elements of law, investigations, ethics, physical security, and business continuity and disaster recovery.

Sumner and Werner's (1997) research examined information systems ethics in a networked environment as part of an information security curriculum. They believed that ethical issues attracted increased attention in the past few years. They categorized ethical issues into privacy, accuracy, property, and accessibility. Privacy dealt with what information a person must reveal to others. Accuracy identified who was responsible for authenticity of the information. Property considered who owns the information, as well as fair price for the use of the information. Accessibility was the information someone has the right to retrieve, under what conditions, and with what safeguards. Using survey research Sumner and Werner (1997) found that management information systems (MIS) professionals demonstrated a greater sensitivity to information systems ethical issues than college students.

Similar to many organizations, academic computing enjoyed rapid growth. In many colleges and universities academic computing consisted of multiple open access computers and computerized classrooms which provided access to a shared network drive, the internet, e-mail servers, library databases, and printing. According to Sumner and Werner (1997) some of the problems that occurred regularly in a networked environment were:

- 1) Abuse of public computing resources, including tying up open-access workstations, disk space, network printers, and other shared resources.
- 2) Invasion of privacy, such as gaining unauthorized access to other people's electronic mail, by breaking passwords or spoofing.
- 3) Improper use of computer systems, including harassment, commercial use of instructional facilities, and misrepresentation of user communications (p.1).

These problems were supposedly addressed by acceptable use policies (AUP); however, in many educational institutions the question of restrictions, consequences, and punishments were less clear and not understood. It was extremely important that

educational institutions educated electronic learners with regard to their rights and responsibilities. This included providing knowledge of the electronic privacy policies that existed. In a statement included in the American Association for Higher Education's (AAHE) *Bill of Rights and Responsibilities for Electronic Learners* the issue of privacy was addressed:

- 1) Since the electronic community of learners is based upon the integrity and authenticity of information, it shall be each citizen's personal responsibility to be aware of the potential for and possible affects of manipulating electronic information, to verify integrity and authenticity, and to assure the security of information that he or she compiles or uses.
- 2) Each citizen, as a member of the electronic community of learners, is responsible to all other citizens in that community, to respect and value the rights of privacy for all, to recognize and respect the diversity of the population and opinion in the community, to behave ethically, and to comply with legal restrictions regarding the use of information resources (Sumner & Werner, 1997, p.1).

Questions of ethics in information systems were prevalent in the computer industry. However, the information systems profession had not raised attention to the broader aspects of the social and ethical impacts of information technology. The prevalence of software piracy, satellite interceptions, hacker intrusions, implanted bugs, viruses, Trojan horses, and trap doors indicated that ethics and the management of information technology were contradictory terms (Sumner & Werner, 1997).

In general, the students were more lenient than the information systems practitioners in which the intent was not malicious. However, Sumner and Werner (1997) found:

on a number of issues the students and practitioners were in agreement on a number of unacceptable behavior including: 1) tying up a computer by playing games when another student needed to do homework, 2) not destroying pirated software, 3) intentionally swamping a mail hub, 4) spreading a destructive virus, 5) mimicking a high-ranking official on the network without explanation, and 6) copying another student's file without authorization (p.6).

The research demonstrated the need for integrating concepts of ethics in information systems education.

Rapid advances in information systems gave users enormous capabilities to process, store, and transmit digital data. This capability increased the requirement for managing information security. In addition to confidentiality, integrity, and availability the principles of responsibility, personal integrity, trust, and ethicality also held the key for successfully managing information security. While technical controls were vital, the uses of information had to be considered (Sumner & Werner, 1997).

The degree of internetworking has transformed traditional centralized, hierarchical organizations into a loosely coupled network of departments and functions characterized by cooperation instead of autonomy and control. This structure facilitated the sharing of information, as well as interpersonal and inter-organizational connectivity. In order to be efficient, effective, and responsive, organizations gave prominence to the use of networks and computer based information systems. Fearing competitive pressure, organizations embraced information technology without regard to the planning or implementation of information security (Dhillon & Blackhouse, 2000).

In light of this evolving information technology environment the role of information security was changing. The focus has shifted to the organization as a whole and the soundness of the information systems. As information systems are operated by people Dhillon and Blackhouse (2000) proposed “what we need are principles that require observance at all times, and especially when there may not be any relevant rules to follow”. Traditional computer science programs had little to offer in this regard.

Curriculum in information security needed to include organizational theory, management science, and emerging technologies in information systems. Information systems security had to address not just the data, but the changing organizational context in which it was interpreted and used (Dhillon & Blackhouse, 2000).

Along with the traditional information security principles of confidentiality, integrity, and availability information security should have included responsibility, personal integrity, trust, and ethicality. Dhillon and Blackhouse (2000) defined these new principles as follows:

1. Responsibility is the understanding of roles and responsibilities inherent in a job. Employees are expected to develop work practices on a basis of a clear understanding of their responsibilities.
2. Personal integrity evaluates how a member of an organization divulges proprietary information to a third party. Business-sensitive information has great value, and organizations need to consider whom they allow to enter the fraternity.
3. Trust is where the emphasis is less on external control and supervision and more self control and responsibility.
4. Ethicality presupposes that fellow members will act in accordance with some ethical practices that are not company rules and can be applied to all formalized procedures (p.38).

Technical controls were vital with regard to users who accessed systems, but new concepts of information security should have considered the behavioral aspects involved with organizational change (Dhillon & Blackhouse, 2000). Research indicated new information security programs must include aspects of management, behavior, law, and business.

Many professional organizations have recommended model curriculum guides used by schools, colleges and universities in the design of programs in information technology. The Joint Task Force on Computing Curricula, comprised of members from both the IEEE Computer Society and the Association for Computing Machinery, developed the

curricula model *Computing Curricula 2001 in Computer Science* which identified a computer science body of knowledge with core topics. This body of knowledge consisted of 132 topics of which four were security related (“The Joint Task Force”, 2001). Office Systems Research Association (OSRA) has redefined its model curriculum for organization and end-user information systems, has recognized the need for an introductory course in information systems security, and has conducted research on a common body of knowledge required for this course (S. Hunt, personal communication, February 20, 2003).

The need for rigorous and scholarly research into the development of an information security curriculum was further emphasized by Longmore-Etheridge’s (2000) paper describing the Fourth Annual Academic/Practitioner Symposium, which convened to create an undergraduate/graduate curriculum model for an area of concentration in information security. This symposium consisted of 40 experts from the field, whose goal was to develop six to eight three credit courses for an information security concentration. Although a survey was used to develop a baseline for the course development it was neither rigorous nor empirical in nature.

In information security two models of information security education were apparent. These models were provided by:

- 1) Private certifying organizations such as the federal government, International Information Systems Security Certificate Consortium, Systems Administration, Network and Security and the International Association of Computer Investigations Specialist; and
- 2) Proprietary sources.

The International Information Systems Security Certificate Consortium (ISC<sup>2</sup>) model represented and attempted to standardize information security into a Common Body of Knowledge (CBK) (Logan, 2002). This organization's CISSP examination was an attempt to ensure that information systems security professionals met standard criteria of knowledge and continued to upgrade that knowledge (Krutz & Vines, 2001).

The University of Maryland recognized the CISSP as being instrumental in identifying a common body of knowledge for implementation in its business management curriculum. Although Hazari (2002) admitted that it did not provide sufficient course work in finance, organization or strategy, it did lay the ground for basic information security.

Kim and Choi (2002) came close to identifying the work actually performed by information systems security professionals in the field. Their research on identifying the educational requirements for information systems security professionals in Korea identified the following as essential for practitioners of information security. In order of importance they were:

- 1) establishing information security policy
- 2) establishing managerial security measures
- 3) analyzing security environments
- 4) risk analysis and assessment
- 5) understanding basic cryptology
- 6) acknowledging laws and regulations
- 7) testing vulnerabilities in information security systems
- 8) designing physical security measures
- 9) coping with hacking
- 10) managing intrusion check and detection
- 11) privacy and ethics
- 12) handling computer viruses
- 13) knowledge of information security standards
- 14) managing security education programs
- 15) knowledge of security system evaluation (p.250).

The determination of key educational requirements for information systems security professionals by security experts was an important contribution to the improvement of information security program development (Kim and Choi, 2002). Kim and Choi's (2002) study gave impetus to the need for more rigorous and empirical research in defining the skills and attributes of information system security professionals in the field.

### **Summary**

The introduction contained procedures for identifying, reviewing, and documenting applicable research completed in the field of information security, information security requirements, and information security curriculum. An historical overview documented information security and education beginning in the 1960s. This section also identified the areas most pertinent to the objectives and goals of this literature search which included:

- 1) Information Technology
- 2) Information Systems Security
- 3) Certification
- 4) Curriculum Design
- 5) Information Systems Security Curriculum

Since rigorous and empirical research is beyond the scope of many research projects, most of the examined documented research addressed only limited information security requirements, or relied on existing and outdated certification or training standards.

Although there were a number of certifications, many were vendor specific. While there were some broad, non-vendor specific certifications the CISSP was considered the only top-down approach to identifying specific requirements and was considered by



many to be the defacto certification. Research indicated information security curriculum fitting into two broad categories:

- 1) developed using the expertise of faculty, or
- 2) based on the training standard identified by NSA in its Centers of Academic Excellence in Information Assurance program.

Both categories did not consider the actual requirements of information systems security professionals in an information systems security work environment. The review of literature supported the need for a rigorous and empirical study to determine the actual tasks performed in an information systems security work environment and to compare these requirements to existing curriculum.

## Chapter 3

### Methodology

Kim and Choi (2002) stated that the determination of key educational requirements for information systems security professionals by experts in the field was important in the development of an information security curriculum. Golshani, et al. (2001) observed that a formal definition of the basic principles of information security did not exist and that this lack contributed to an unstructured approach to information security. As of 2002, information systems curriculum was driven by the NSA Centers of Academic Excellence in Information Assurance Education. The award of this designation was dependent upon meeting 10 specific criteria for measurement. The first criteria for designation mandated that the academic program of the university be tied to NSTISSI 4011; however, none of the criteria for this designation evaluated the skills and attributes currently employed in an information systems security work environment.

This research performed a rigorous review of information systems security skills and attributes and provided answers to the following questions:

- 1) Are the skills and attributes identified in the CISSP employed in an information systems security work environment?
- 2) Are universities designated as NSA Centers of Academic Excellence in Information Assurance Education providing these skills?

These questions were answered by the examination of the 10 CISSP domains from within the information systems security work environment to determine which skills were necessary and the examination of existing NSA Centers of Academic Excellence in Information Assurance Education curriculum to determine which skills and attributes from within the 10 domains were being taught. Using empirical methods the goal of this research was to determine if existing curriculum in colleges and universities designated as NSA Centers of Academic Excellence in Information Assurance Education was consistent with the needs of an information systems security work environment.

The null hypotheses tested were:

- 1)  $H_01$ : The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment.
- 2)  $H_02$ : There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education.

## **Research Methods**

Data collection was accomplished by using sampling survey research. In the design of this research two issues were addressed: 1) identifying a sufficient sample size, and 2) instrument reliability and validity.

In their article on determining sample size Bartlett, Kotrlik, and Higgins (2001) listed four ways of estimating population sample size: 1) take the sample in two steps, and use the results from the first to determine the number of additional samples needed, 2) use a pilot study, 3) use data from a previous study, or 4) use logical mathematical formulas to

estimate the size. They included a table for determining minimum required sample sizes based on mathematical formulas, which used a margin of error of .03, an alpha of .05, and a  $t$  of 1.96. Using Bartlett, et al.'s (2001) table the minimum required responses for a sample size from a population of 4,700 was 119. To ensure a representative return rate this research selected 800 respondents in a randomly sorted list of information systems security professionals.

There were 323 faculty members in the target population. Bartlett, et al. (2001) identified 85 responses as being representative of a population numbering 300. To ensure an adequate sample size, all 323 respondents were surveyed.

#### *Procedures Used to Develop the Survey*

The data used in this descriptive study was collected through a researcher developed survey. The survey method of data collection was chosen over the interview method due to geographic distribution of the population. The following procedures were used to develop the survey instrument: 1) develop the conceptual framework, 2) develop the operational definitions, 3) select the scaling technique, 4) review of items, 5) develop response format, 6) develop directions, 7) prepare draft and distribute pilot, 8) analyze pilot data and revise instrument (if required), 9) produce instrument, 10) conduct reliability and validity analysis, and 11) distribute survey (Bartlett, et al. 2001).

#### Develop the Conceptual Framework

The Information Systems Security Certification Consortium (ISC)<sup>2</sup> was instrumental in the development of the Certified Information Systems Security Professional (CISSP), which was considered the most comprehensive certification for information systems security professionals (Dugan & Prencipe, 2001). Although CISSP was not the only

certification available for information systems security professionals it was the only broad top-down certification covering theoretical knowledge of 10 domains, with specific tasks recognized to be required for information security certification. It was this theoretical requirement that was selected as the baseline to identify skills and attributes for a common body of knowledge in information security and to identify whether academia was providing education in this common body of knowledge.

### Develop the Operational Definitions

The CISSP domains cover the following areas of information security responsibilities:

1) *Access Control Systems and Methodology*, 2) *Telecommunications and Network Security*, 3) *Security Management Practices*, 4) *Applications and Systems Development Security*, 5) *Cryptography*, 6) *Security Architecture and Models*, 7) *Operations Security*, 8) *Business Continuity Planning and Disaster Recovery Planning*, 9) *Laws, Investigations, and Ethics*, and 10) *Physical Security*. The CISSP domains were chosen as the defining criteria for the development of the operational definitions after an extensive review of literature which included research studies, journal articles, books, and text books in the field of information security.

### Select the Scaling Technique

Scales typically are used to obtain responses that will be comparable to one another. This research used a verbal frequency scale which differed from the Likert in that it indicated how often an action had been taken. According to Alreck and Settle (1995) there were two incentives to using verbal frequency scaling: 1) the ability to array activities across a multiple category spectrum for data description, and 2) the ease of making comparisons among different actions for the same sample of respondents. This

research was concerned with the frequency of use of specific skills within the information systems security professional's work environment and the frequency of teaching these skills in an academic environment. The scaling of: 1) always, 2) often, 3) sometimes, 4) rarely, and 5) never, was deemed an acceptable frequency range for this research.

### Review of Items

According to Alreck and Settle (1995) effective survey questions have three defining characteristics: 1) focus, 2) brevity, and 3) simplicity. The initial review of the CISSP domains identified 63 specific skills and attributes in which information systems security professionals should be proficient. Although 63 questions met the characteristic of focus, it fell short in brevity and simplicity. A thorough review of the CISSP domain descriptions identified specific categories where identified skills and attributes could be combined without losing focus. The breakdown of the 63 questions was accomplished during an initial pilot survey committee (see Appendix A) meeting. These combined skills and attributes allowed the development of a 24 question survey in the following categories:

Domain 1, *Access Control Systems and Methodology*, requires competencies in the following skills: 1) access control techniques and administration including mandatory access control, discretionary access control, and non-discretionary access control and combinations, 2) access control models including Bell-Lapadula, Biba, Clark and Wilson, Non-Interference, State Machine, and Access Matrix and Information Flow Model, 3) identification and authentication techniques such as knowledge based password, Personal Identification Numbers (PINs), characteristic-based, tokens, tickets, one-time passwords, biometrics, and single sign-on, 4) access control methodologies including

centralized/remote authentication and decentralized access controls, 5) file and data ownership and custodianship, 6) methods of attack, 7) intrusion, and 8) penetration detection. These skills were combined to form four questions relating to Domain 1.

Domain 2, *Telecommunications and Network Security*, requires competencies in the following skills: 1) International Standards Organization, 2) Open Systems Interconnection layers and characteristics, 3) communications and network security, 4) Internet/Intranet/Extranet, 5) E-mail security, 6) facsimile security, 7) secure voice communications, 8) security boundaries, 9) policy and controls, and 10) network attacks and countermeasures. These skills were combined to form one question relating to Domain 2.

Domain 3, *Security Management Practices*, consists of the following skills: 1) security management concepts and principles, 2) change control and management, 3) data classification, 4) employment policies and practices, 5) policies, 6) standards, guidelines and procedures, 7) roles and responsibilities, 8) security awareness training, and 9) security management. These skills were combined to form three questions relating to Domain 3.

Domain 4, *Applications and Systems Development Security*, consists of the following skills: 1) application issues, 2) database and data warehousing, 3) data and information storage, 4) knowledge based systems, 5) systems development controls, 6) malicious code, and 7) methods of attack. These skills were combined to form two questions relating to Domain 4.

Domain 5, *Cryptography*, consists of the following skills: 1) cryptographic concepts, 2) methodologies and practices, 3) private key algorithms, 4) public key algorithms,

5) public key infrastructure, 6) system architecture for implementing cryptographic functions, and 7) methods of attack. These skills were combined to form two questions relating to Domain 5.

Domain 6, *Security Architecture and Models*, consists of the following skills: 1) principles of common computer and network organizations, 2) architectures and design, 3) principles of common security models, 4) architectures and evaluation techniques, 5) common flaws and security issues associated with confidentiality, integrity, and availability, and 6) systems architecture and design. These skills were combined to form three questions relating to Domain 6.

Domain 7, *Operations Security*, consists of the following skills: 1) administrative management, 2) security concepts, 3) control types, 4) operations controls, 5) resource protection, 6) audit trails, 7) monitoring tools and techniques, 8) intrusion detection, 9) penetration detection techniques, 10) inappropriate activities, threats, counter measures, and 11) violations, breaches and reporting. These skills were combined to form two questions relating to Domain 7. One question was later identified by the validity process as being unnecessary and was removed leaving only one question relating to Domain 7.

Domain 8, *Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)*, identifies skills to counteract interruptions to business activities and protect critical business processes from the effects of major failures or disasters. These skills were combined to form two questions relating to Domain 8.

Domain 9, *Laws, Investigations and Ethics*, consists of the following skills: 1) major categories and types of laws, 2) investigations, 3) major categories of computer crime and



incident handling, and 4) ethics. These skills were combined to form three questions relating to Domain 9.

Domain 10, *Physical Security*, consists of the following skills: 1) facility requirements, 2) technical controls, 3) environment/life safety, 4) physical security threats, and 5) elements of physical security. These skills were combined to form two questions relating to Domain 10.

### Develop Response Format

The survey response format consisted of two parts: 1) validation data, and 2) competencies data.

The validation section obtained professional background data from the survey respondents. It ensured that participants met the requirements to complete the survey. A “no” response in this section sent the participant to an exit page.

In the competency section the 24 statements were listed. The competency statements were later reduced to 23 by the validity process. The respondents were asked to rate each statement according to its use in an information systems security environment (for the information systems security professional survey) or teaching in an information systems security curriculum (for the information systems security faculty survey). Each question had a verbal frequency response consisting of: 1) all the time, 2) some of the time, and 3) never, which was later changed during the pilot phase to: 1) always, 2) often, 3) sometimes, 4) rarely, and 5) never, identified by a radio button corresponding to a linear numeric scale and assigned to a discrete table in a database, which provided interval data. Defining each question as a discrete field in this table allowed: 1) the data to be easily separated for compilation and analysis, and 2) the capture of data from partial

completions. This allowed the use of the skills in a work environment, as determined by information systems security professionals, to be compared to the teaching of the skills in an information systems security curriculum.

### Develop Directions

The directions informed the respondent how to respond to the question. According to Alreck and Settle (1995), the minimum directions a survey should include are: 1) what items to rate, 2) what standard to use, 3) how to use the scale, and 4) how to record the responses. It is better to provide more thorough instructions to ensure all respondents understand what is needed. There were no special instructions required in this research.

### Prepare Draft and Distribute Pilot

Using the scaling techniques, operational definitions, and directions a draft survey was prepared (see Appendix C), as a pilot, for distribution to six Information Systems faculty from Bloomsburg University of Pennsylvania.

The cover letter (see Appendix B), the pilot survey (see Appendix C), the evaluation procedures (see Appendix D) and comments and responses (see Appendix E) were distributed to six Information Systems faculty members from Bloomsburg University of Pennsylvania (see Appendix A ), consisting of one full professor, four associate professors and one assistant professor, each familiar with information security concepts. The pilot survey used the following specific questions, identified by Litwin (1995), as being essential in a pilot study:

- 1) Were there any typographical errors?
- 2) Were there any misspelled words?
- 3) Did the numbers make sense?

- 4) Was the type size big enough to easily read?
- 5) Was the vocabulary appropriate for the respondents?
- 6) Was the survey too long?
- 7) Was the style of the items too monotonous?
- 8) Did the survey format flow well?
- 9) Were the items appropriate for the respondents?
- 10) Were the items sensitive to possible cultural barriers?
- 11) Was the survey in the best language for the respondents? Of further interest to this research were the questions: 1) Did the survey adequately address the skills in an information systems security environment? 2) Were there any skills that should be added? 3) What was the time for completion?

All six committee members completed the survey in the same manner as the actual population in the study was requested to do.

#### Analyze Pilot Study and Revise Instrument (if required)

The pilot survey was analyzed to identify errors in form or presentation, or identify shortcomings within the questions. The survey was changed to address these issues and then re-administered to the pilot survey committee for additional comments. Upon finishing the survey, the committee members were interviewed individually to ascertain their reaction and comments. As a result of the pilot survey minor changes in format and content were made.

#### Produce Instrument

At the completion of the successful pilot survey the instrument was produced in a form suitable for reliability and validity testing.

### Conduct Validity and Reliability Analysis

The survey was reviewed for both face and content validity. Litwin (1995) described face validity as the casual review of how good an item or group of items appear, while content validity is a formal review by experts in some aspect of the subject under study.

In face validity the survey, cover letter, and comment sheet were distributed to five Business Education/Office Information Systems faculty members from Bloomsburg University of Pennsylvania (see Appendix F), consisting of two full professors, two associate professors, and one assistant professor, each having performed and published survey research. A meeting was held with the face validity committee and the surveys discussed. At the completion of the face validation meeting, minor changes in format and grammar were made.

Content validity was evaluated by using a panel of 100 experts, drawn randomly from the population of information systems security professionals, who were considered to have knowledge and/or skills in information security by virtue of their CISSP certification. This random panel of 100 experts was removed from the population.

**Table 1, Qualifications of Content Validity Panel**

<b>Members holding CISSP certification</b>	<b>Members publishing articles pertaining to information security</b>	<b>Members presenting papers pertaining to information security</b>
99	35	58

This research used a modified Delphi technique to assess the content validity of the survey. The modified Delphi approach consisted of identifying a select group of information systems security professionals who, by successive rounds, collaborated on

the development of a survey to identify specific competencies, taken from the CISSP exam, in use in an information systems security work environment. These 100 randomly selected information systems security professionals were contacted via e-mail. Thirty-five e-mails were returned as invalid addresses. Of the remaining 65 valid e-mails, 18 (27%) responded to the request to participate in the content validity review.

In round one of the content validity phase, access to the survey was provided to the 18 reviewers (see Appendix G). The survey identified 24 information security questions based on the CISSP domains (see Appendix H). These questions used a five point verbal frequency as follows: 1) always, 2) often, 3) sometimes, 4) rarely, and 5) never. The survey was set up on a secure Web site with a validation page to ensure the reviewers met specific requirements. These requirements were: 1) published textbook(s) or article(s) in the area of information security, 2) participation in at least one national or state convention as a speaker or panel member discussing the topic of information security, 3) a member of the faculty of an accredited university with a viable information security curriculum, or 4) held a CISSP certification. Of the 18 reviewers 100% held CISSP certifications, three (16%) had published textbooks or articles pertaining to information security, and three (16%) had participated in at least one national or state convention as a speaker or panel member discussing the topic of information security. Each of the reviewers was asked to rate the questions as follows: 1) the question correctly identifies the need, 2) the question is incorrectly stated; needs revision or 3) do not use, competency inappropriate. A section for reviewer comments was provided. To facilitate statistical analysis the reviewer scale was assigned the following weights: 1) three points for correctly identifies the need, 2) two points for incorrectly stated; needs revision, and

3) one point for do not use, competency inappropriate. Any question in which 20% or more of the reviewers felt the question needed revision and/or the mean and the lower limit of the confidence interval fell below 2.5, on a scale of 1 to 3, was considered incorrectly stated and was revised for submission to the reviewers in round two. Any question in which 70% or more of the respondents stated the question inappropriate was removed from the survey.

The results of round one (see Appendix I) were analyzed using the Statistical Package for Social Science (SPSS). The statistics used for analysis determined the Mean, Standard Deviation (SD), Standard Error of the Mean (SE), and a 95% Confidence Interval (CI). As a result of this analysis question 23 was removed from the survey and questions 5, 14, and 20 were revised and submitted to round two.

In round two of the content validity phase an e-mail (see Appendix J) was sent to 18 validity committee members of whom 16 responded. Two responses were returned as invalid e-mails so no reminder e-mails were sent. The round two content validity survey (see Appendix K) was set up on a secure Web site. Each of the validity committee members were asked to rate the questions as: 1) accept the revision, no comments, 2) accept the revision, with comments or 3) reject the revision, with comments. A section for reviewer comments was provided. To facilitate statistical analysis the reviewer scale was assigned the following weights: 1) three points for accept the revision, no comments, 2) two points for accept the revision, with comments, and 3) one point for reject the revision, with comments. As a result of round two (see Appendix L) the revisions of questions 5, 14, and 20 were accepted.

In the reliability phase the survey was tested for split-half reliability. The split-halves method consisted of administering the survey to 200 randomly selected members of the population, who were then removed from the population as a whole, and split in half for scoring. The procedure used obtained a score based on the odd numbered items in the test and a score based on the even numbered items in the test for each individual response. The correlation coefficients between the odd and even numbered scores were then calculated. This correlation coefficient, however, was not the reliability coefficient of the test. The total test was twice as long as each half, so an adjustment was made to obtain the reliability of the total test. Litwin (1995) stated the split-halves method "is generally accepted as being as good as administering the different forms to the same sample at different time points".

These 200 randomly selected information systems security professionals were contacted via e-mail (see Appendix N). Forty-one e-mails were returned as invalid addresses. Of the remaining 159 valid e-mails sent, 16 (10 %) responded and completed the reliability survey. Because of the low response rate a second e-mail was sent ten days after the initial request. The responses from the first e-mailing were gathered into a database, and an initial query was run to identify and remove the invalid responses from the respondent sample. An additional query was developed to identify those subjects who had responded and remove them from the sample. The remaining population samples were then identified as non-respondents and were selected to receive the reminder e-mail (see Appendix N). This second e-mailing resulted in an additional 10 responses to bring the total to 26 (16%). Of the 26 reviewers 100% held CISSP certifications, four (15%) had published textbooks or articles pertaining to information security, and ten (38%) had

participated in at least one national or state convention as a speaker or panel member discussing the topic of information security. The instrument was deemed to be reliable based on the split-halves method (see Table 1). Using SPSS to perform the split-halves computation the following results were noted: Guttman split-half = .8572, unequal-length Spearman-Brown = .8614.

**Table 2, Split-halves Results for Reliability Phase  
Reliability Coefficients**

N of Cases = 26	N of Items = 23
Correlation between forms = .7562	Equal-length Spearman-Brown = .8612
Guttman split-half = .8572	Unequal-length Spearman-Brown = .8614
12 Items in part 1	11 Items in part 2
Alpha for part 1 = .8334	Alpha for part 2 = .8719

To confirm the split-halves reliability, a computation of Cronbach's was performed (see Table 3). The standardized alpha for the 23 question scale was 0.9141, indicating a high degree of internal consistency.

**Table 3, Cronbach's Alpha  
Reliability Analysis**

Reliability Coefficients

N of Cases = 26.0	N of Items = 23
Alpha = .9141	



The individual scale item statistics confirmed this finding of a high degree of internal consistency, with all items exhibiting a positive Corrected Item-Total Correlation. Because deleting any item would have no significant effect on the overall scale reliability, all 23 items were justified for retention.

### Distribute Surveys

Both surveys were made available on a secure Web server using forms developed using Microsoft FrontPage®. The responses from these forms were sent to a database on the Web server with separate tables for each of five response areas: 1) information systems security faculty validation, 2) information systems security professionals validation, 3) information systems security faculty survey, 4) information systems security professionals survey, and 5) respondent's request for survey results. Responses were tracked using randomly assigned Personal Identification Numbers (PINs). At the conclusion of data collection all references relating PINs to e-mail addresses were deleted in compliance with IRB (see Appendix M) requirements.

From the sample of 4700 (=N) information systems security professionals a random sample of 800 (=n) was drawn. There were 165 invalid e-mail addresses identified. Subtracting the invalid e-mail addresses provided a usable sample of 635. There was a non-response rate of 80%. The non-respondents did not differ from the respondents with regard to important characteristics. The statistical analyses had taken into account both the sampling design, and the response probabilities. The initial survey e-mail was distributed on November 21, 2003. This distribution resulted in a return of 94 (14%). A second reminder e-mail was distributed on December 1, 2003. This distribution resulted in an additional 27 responses bringing the total to 121 (19%). A third reminder e-mail

was distributed on December 11, 2003. This distribution resulted in an additional four responses for a total response of 125 (20%).

The validation process was developed to ensure that only CISSP certification holders completed the survey. Of further interest to this research were the number of respondents who had published books or articles relating to information security, the number of respondents who had participated as panel members in conferences relating to information security, and the number of respondents who had presented papers relating to information security. Of the respondents 125 (100%) held CISSP certifications, 34 (27%) had published articles or books relating to information security, 51 (40%) had participated as panel members in discussions relating to information security, and 3 (.03%) had presented papers relating to information security.

From the sample of 321 (N) information systems security faculty the total 321 (n) were used. There were 20 invalid e-mail addresses identified. Subtracting the invalid e-mail addresses provided a usable sample of 301. There was a non-response rate of 67%. The non-respondents did not differ from the respondents with regard to important characteristics. The statistical analyses had taken into account both the sampling design, and the response probabilities. The initial survey e-mail was distributed on November 21, 2003. This distribution resulted in a return of 60 (20%). A second reminder e-mail was distributed on December 1, 2003. This distribution resulted in an additional 36 responses bringing the total to 96 (31%). A third reminder e-mail was distributed on December 11, 2003. This distribution resulted in an additional three responses bringing the total to 99 (33%).

The validation process was developed to ensure that only faculty teaching in NSA Schools of Excellence in Information Assurance completed the survey. Of further interest to this research were the number of respondents who held a CISSP certification, the number of respondents who had published books or articles relating to information security, and the number of respondents who had presented papers relating to information security. Of the respondents 99 (100%) were teaching in NSA Schools of Excellence in Information Assurance, 6 (6%) held a CISSP certification, 35 (35%) had published articles or books relating to information security, and 58 (59%) had presented papers relating to information security.

## **Discussion**

Collecting data via a Web based survey eliminated the data input stage required in paper samples; however, care was taken to ensure that the Web based surveys were accessible to all. During data collection one respondent had trouble initially completing the survey due to using an Apple based browser. The Web site was reconfigured to accept all browsers allowing this respondent to complete the survey.

This research indicated that both information systems security professionals (27%) and information systems security faculty (35%) were active in publications relating to information systems security; however information systems security faculty (59%) presented more often than information systems security professionals (.03%). Panel membership (40%) was high among information systems security professionals, while CISSP certification (6%) was low among information systems security faculty.

## Formats for Presenting Results

The database results were exported to an Excel spreadsheet. The raw spreadsheet data (see Appendix R) was then migrated to SPSS for analysis. Data analysis required the use of statistical tools to reduce the amount of detail collected, summarizing it and making the most important facts and relationships apparent.

As the data from each survey question was considered a variable this research began the analysis with univariate statistics. The data comparing the competencies taught against the competencies required used bivariate statistics.

Initially, this research used frequency and percentage tables to evaluate the distribution of responses. In order to identify the appropriate statistical tool the scale of the data was first identified. In this research the data collected was considered to be an interval scale as the interval between scale points was equal. As such the descriptive statistics included the mean, median, and mode. The spread identified the standard deviation, range, maximum, and minimum. The shape identified skewness and kurtosis. This research assumed a 95% confidence level to ensure a valid degree of reliability.

As the data was identified as interval, the statistical measure of association between what was taught and what was required evaluated the data using discriminate analysis and correlation of analysis. As no causality was implied and the focus was strictly on the degree of association, this research did not designate dependent and independent variables.

The specific tools for the analysis of the taught and required consisted of: 1) cross-tabulation which indicated the relationship between variables without the need for

dependent or independent variable identification, and 2) correlation analysis which showed how much the two variables moved together.

### **Resource Requirements**

There were no additional resource requirements. The survey was deployed on an existing educational Web site. All participants were notified via e-mail.

### **Summary**

This research examined the correlation between competencies employed in an information systems security work environment and the competencies taught in academic institutions designated as NSA Centers of Academic Excellence in Information Assurance Education.

Data collection was accomplished using sampling survey research. In the design of the sampling survey two issues were addressed: 1) identifying a sufficient sample size, and 2) instrument reliability and validity.

The information systems security faculty survey (see Appendix O) consisted of two sections: 1) validation data, and 2) competencies data. The validation section ensured participants were currently teaching, or had taught an information systems security course. Each question in the CISSP competencies area was assigned to a discrete table in the faculty database. Each question had a response identified by a radio button corresponding to a linear numeric scale which provided interval data. The submission of each response sent the participant to the next question. At this point the participant was advised of the number of remaining questions.

The information systems security professional survey (see Appendix P) consisted of two areas: 1) validation data, and 2) competencies data. The validation section ensured

participants were currently working in an information systems security work environment and held a CISSP certification. Each question in the CISSP competencies area was assigned to a discrete table in the information systems security professional database. Each question had a response identified by a radio button corresponding to a linear numeric scale which provided interval data. The submission of each response sent the participant to the next question. At this point the participant was advised of the number of remaining questions.

## Chapter 4

### Results

The first section of this chapter describes the statistical tools used to analyze the results of this research. The second section is the statistical analysis and findings of the comparisons of each of the questions answered by information systems security professionals in a survey with a comparison to the ten domains of the CISSP. This section also statistically compares the results of the questions answered in a survey by information systems security professionals to the results of the questions answered in a survey by information systems security faculty to ascertain any degree of association between the two. The final section summarizes the results of the analysis of both the comparisons to the CISSP and the degree of association between what was taught at NSA Centers of Academic Excellence in Information Assurance Education and what was employed in the information systems security work environment.

#### **Statistical Tools Used in Analysis**

The research questions were:

- 1) Are the skills and attributes identified in the CISSP employed in an information systems security work environment?
- 2) Are universities designated as National Security Agency Centers of Academic Excellence in Information Assurance Education providing these skills?

The null hypotheses tested were:

- 1)  $H_{01}$ : The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment.
- 2)  $H_{02}$ : There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education.

All questions were evaluated using measures of central tendencies and inferential statistics. The Chi Square was used to test the statistical significance of differences of the relationship between what information systems security professionals employed and what information systems security faculty taught (two-way classification). If the calculated P-value was less than 0.05, then there was a statistically significant relationship between the two classifications.

The ordinal data in this study was tested for significance using the Kendall's tau-b and the Wilcoxon-Matched-Pairs Signed-Ranks statistical tests. The Kendall's tau-b statistic test was used as a measure of agreement between what information systems security professionals employed and what information systems security faculty taught. The Wilcoxon-Matched-Pairs Signed-Ranks test is typically used to compare the averages of two independent groups. Using the  $z$  score and the  $p$  value this statistic was used to test the difference between the two groups. The measures of central tendencies and skewness of the questions were employed to evaluate hypothesis  $H_{01}$ : The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment. The Chi-Square, Kendall's tau-b and Wilcoxon Matched-



Pairs Signed-Ranks tests were used to evaluate hypothesis Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education. The level of significance was set at 0.05 for rejection of the null hypothesis. The data was evaluated using Statistical Package for Social Science (SPSS), a computer based statistical analysis program. The results of the analysis of the employment and teaching of the domains of the CISSP follow. The printouts from the statistical analysis program are contained in Appendix Q.

### **Statistical Analysis and Findings**

#### *Domain 1 Analysis*

Four questions were used to evaluate Domain 1, *Access Control Systems and Methodology*. For information systems security professionals these questions were designated:

1. Pro1, how often do you employ access control techniques, access control administration, and access control models?
2. Pro2, how often do you employ identification and authentication techniques?
3. Pro3, how often do you employ intrusion detection monitoring and penetration testing?
4. Pro4, how often do you employ International Standards Organization/Open Systems Interconnection, layers and characteristics?

For information systems security faculty these questions were designated:

1. Edu1, how often do you teach access control techniques, access control administration, and access control models?

2. Edu2, how often do you teach identification and authentication techniques?
1. Edu3, how often do you teach intrusion detection monitoring and penetration testing?
2. Edu4, how often do you teach International Standards Organization/Open Systems Interconnection, layers and characteristics?

The scaling of the survey was as follows: always (5), often (4), sometimes (3), rarely (2), and never (1).

According to the descriptive statistics access control techniques, access control administration, and access control models (pro1) with a mean (M) of 4.6080 were employed more than access control techniques, access control administration, and access control models (edu1) with a mean of (M) of 3.7172 were taught. The negative skewness of pro1 (-1.550) and edu1 (-.839) indicated a greater number of larger values. The small standard error of mean indicated the means of pro1 (SE = .05553) and edu1 (SE = .13005) were good estimators of the population mean and indicated the null hypothesis, Ho1: The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, was not rejected.

Although information systems security professionals employed access control techniques, access control administration, and access control models (pro1) to a greater extent than information systems security faculty taught access control techniques, access control administration, and access control models (edu1) the Chi-Square test showed no statistically significant correlation ( $\chi^2 (9, N = 99) = 2.843, P = .970, P > .05$ ) which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work

environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

Kendall's tau-b analysis of the employment of access control techniques, access control administration, and access control models (pro1) and the teaching of access control techniques, access control administration, and access control models (edu1), ( $t(N = 99) = -.013$ ,  $t < .10$ ) indicated no statistically significant association which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

The descriptive statistics indicated the means of the employment of access control techniques, access control administration, and access control models (pro1) and the teaching of access control techniques, access control administration, and access control models (edu1) were different. The Wilcoxon Matched-Pairs Signed-Ranks, ( $W(N = 99) = -5.486$ ,  $P = .000$ ,  $P < .05$ ) indicated the difference was not coincidental.

According to the descriptive statistics identification and authentication techniques (pro2) with a mean ( $M$ ) of 4.6080 were employed more than identification and authentication techniques (edu2) with a mean ( $M$ ) of = 3.8990 were taught. The negative skewness of pro2 (-.990) and edu2 (-1.220) showed a greater number of larger values. The small standard error of mean indicated the means of pro2 ( $SE = .04580$ ) and edu2 ( $SE = .12639$ ) were good estimators of the population mean which indicated the null hypothesis, Ho1: The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, was not rejected.

Although information systems security professionals employed identification and authentication techniques (pro2) to a greater extent than information systems security faculty taught identification and authentication techniques (edu2) the Chi-Square test showed no statistically significant correlation ( $\chi^2(8, N = 99) = 4.198, P = .839, P > .05$ ) which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

Kendall's tau-b analysis of the employment of identification and authentication techniques (pro2) and the teaching of identification and authentication techniques (edu2), ( $t(N = 99) = .109, t < .10$ ) indicated no statistically significant association which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

The descriptive statistics indicated the means of the employment of identification and authentication techniques (pro2) and the teaching of identification and authentication techniques (edu2) were different. The Wilcoxon Matched-Pairs Signed-Ranks, ( $W(N = 99) = -5.116, P = .000, P < .05$ ) indicated the difference was not coincidental.

According to the descriptive statistics intrusion detection monitoring and penetration testing (pro3) with a mean ( $\underline{M}$ ) of 4.0080 were employed more than intrusion detection monitoring and penetration testing (edu3) with a mean ( $\underline{M}$ ) of 3.7576 were taught. The negative skewness of pro3 (-1.115) and edu3 (-.653) showed a greater number of larger

Although information systems security professionals employed identification and authentication techniques (pro2) to a greater extent than information systems security faculty taught identification and authentication techniques (edu2) the Chi-Square test showed no statistically significant correlation ( $\chi^2(8, N = 99) = 4.198, P = .839, P > .05$ ) which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

Kendall's tau-b analysis of the employment of identification and authentication techniques (pro2) and the teaching of identification and authentication techniques (edu2), ( $t(N = 99) = .109, t < .10$ ) indicated no statistically significant association which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

The descriptive statistics indicated the means of the employment of identification and authentication techniques (pro2) and the teaching of identification and authentication techniques (edu2) were different. The Wilcoxon Matched-Pairs Signed-Ranks, ( $W(N = 99) = -5.116, P = .000, P < .05$ ) indicated the difference was not coincidental.

According to the descriptive statistics intrusion detection monitoring and penetration testing (pro3) with a mean ( $M$ ) of 4.0080 were employed more than intrusion detection monitoring and penetration testing (edu3) with a mean ( $M$ ) of 3.7576 were taught. The negative skewness of pro3 (-1.115) and edu3 (-.653) showed a greater number of larger

values. The small standard error of mean indicated the means of pro3 ( $SE = .08762$ ) and edu3 ( $SE = .12275$ ) were good estimators of the population mean which indicated the null hypothesis,  $H_01$ : The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, was not rejected.

Although intrusion detection monitoring and penetration testing (pro3) was employed to a greater extent than information systems security faculty taught intrusion detection monitoring and penetration testing (edu3) the Chi-Square test showed no statistically significant correlation ( $\chi^2 (16, N = 99) = 17.762, P = .338, P > .05$ ) which indicated the null hypothesis,  $H_02$ : There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

Kendall's tau-b analysis of the employment of intrusion detection monitoring and penetration testing (pro3) and the teaching of intrusion detection monitoring and penetration testing (edu3), ( $t (N = 99) = .052, t < .10$ ) indicated no statistically significant association which indicated the null hypothesis,  $H_02$ : There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

The descriptive statistics indicated the means of the employment of intrusion detection monitoring and penetration testing (pro3) and the teaching of intrusion detection monitoring and penetration testing (edu3) were different. The Wilcoxon Matched-Pairs

Signed-Ranks, ( $W$  ( $N = 99$ ) = -2.096,  $P = .036$ ,  $P < .05$ ) indicated the difference was not coincidental.

According to the descriptive statistics International Standards Organization/Open Systems Interconnection, layers and characteristics (pro4) with a mean ( $M$ ) of 4.1840 were employed more than International Standards Organization/Open Systems Interconnection, layers and characteristics (edu4) with a mean ( $M$ ) of 3.6768 were taught. The positive skewness of pro4 (.347) indicated the response showed a greater number of the middle values while the negative skewness of edu4 (-.691) showed a greater number of larger values. The small standard error of mean confirmed the means of pro4 ( $SE = .04455$ ) and edu4 ( $SE = .10336$ ) were good estimators of the population mean which indicated the null hypothesis,  $H_{01}$ : The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, was not rejected.

Although International Standards Organization/Open Systems Interconnection, layers and characteristics (pro4) were employed to a greater extent than information systems security faculty taught International Standards Organization/Open Systems Interconnection, layers and characteristics (edu4) the Chi-Square test showed no statistically significant correlation ( $\chi^2$  (16,  $N = 99$ ) = 4.410,  $P = .818$ ,  $P > .05$ ) which indicated the null hypothesis,  $H_{02}$ : There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

Kendall's tau-b analysis of the employment of International Standards Organization/Open Systems Interconnection, layers and characteristics (pro4) and the teaching of International Standards Organization/Open Systems Interconnection, layers and characteristics (edu4), ( $t(N = 99) = .104, t > .10$ ) indicated a statistically weak association. This association was significantly low, and combined with the results of the Chi-Square statistic, indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

The descriptive statistics indicated the means of the employment of International Standards Organization/Open Systems Interconnection, layers and characteristics (pro4) and the teaching of International Standards Organization/Open Systems Interconnection, layers and characteristics (edu4) were different. The Wilcoxon Matched-Pairs Signed-Ranks, ( $W(N = 99) = -4.424, P = .000, P < .05$ ) indicated the difference was not coincidental.

### *Domain 1 Findings*

The statistics indicated that information systems security professionals employed the skills and attributes identified in Domain 1 of the CISSP, *Access Control Systems and Methodology*, in an information systems security work environment. The statistical analysis of the questions representing Domain 1 indicated the null hypotheses, Ho1: The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, and Ho2: There is no association between the skills and attributes identified as being employed in an information systems



security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, were not rejected.

Of particular interest is the Kendall's tau-b statistic for pro4 and edu4 ( $t(N = 99) = .104, t > .10$ ) which identified a statistically weak association. The Wilcoxon Matched-Pairs Signed-Ranks statistic indicated the association was not coincidental ( $W(N = 99) = -4.424, P = .000, P < .05$ ). However, the result of the Kendall's tau-b statistic ( $t(N = 99) = .104, t > .10$ ) was significantly small, and combined with the results of the other statistics indicated that the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

### *Domain 2 Analysis*

One question was used to evaluate Domain 2, *Telecommunications and Network Security*. For information systems security professionals this question was designated:

1. Pro5, how often have you employed security controls when addressing communications and network security, Internet/Intranet/Extranet, e-mail security, facsimile security, secure voice communications, and security boundaries?

For information systems security faculty this question was designated:

1. Edu5, how often do you teach security controls when addressing communications and network security, Internet/Intranet/Extranet, e-mail security, facsimile security, secure voice communications, and security boundaries?

The scaling of the survey was as follows: always (5), often (4), sometimes (3), rarely (2), and never (1).

According to the descriptive statistics security controls when addressing communications and network security, Internet/Intranet/Extranet, e-mail security, facsimile security, secure voice communications, and security boundaries (pro5) with a mean (M) of 4.3920 were employed more than security controls when addressing communications and network security, Internet/Intranet/Extranet, e-mail security, facsimile security, secure voice communications, and security boundaries (edu5) with a mean (M) of 3.9596 were taught. The negative skewness of pro5 (-.745) and edu5 (-.676) showed a greater number of larger values. The small standard error of mean indicated the means of pro5 (SE = .06415) and edu5 (SE = .10543) were good estimators of the population mean which indicated the null hypothesis, Ho1: The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, was not rejected.

Although security controls when addressing communications and network security, Internet/Intranet/Extranet, e-mail security, facsimile security, secure voice communications, and security boundaries (pro5) were employed to a greater extent than information systems security faculty taught security controls when addressing communications and network security, Internet/Intranet/Extranet, e-mail security, facsimile security, secure voice communications, and security boundaries (edu5) the Chi-Square test showed the correlation was not statistically significant ( $\chi^2 (6, \underline{N} = 99) = 6.213$   $\underline{P} = .400, \underline{P} > .05$ ) which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

Kendall's tau-b analysis of the employment of security controls when addressing communications and network security, Internet/Intranet/Extranet, e-mail security, facsimile security, secure voice communications, and security boundaries (pro5) and the teaching of security controls when addressing communications and network security, Internet/Intranet/Extranet, e-mail security, facsimile security, secure voice communications, and security boundaries (edu5), ( $t(N = 99) = -.072, t < .10$ ) indicated no statistically significant association, which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being used in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

The descriptive statistics indicated the means of the employment of security controls when addressing communications and network security, Internet/Intranet/Extranet, e-mail security, facsimile security, secure voice communications, and security boundaries (pro5) and the teaching of security controls when addressing communications and network security, Internet/Intranet/Extranet, e-mail security, facsimile security, secure voice communications, and security boundaries (edu5) were different. The Wilcoxon Matched-Pairs Signed-Ranks, ( $W(N = 99) = -2.840, P = .005, P < .05$ ) confirmed the difference was not coincidental.

### *Domain 2 Findings*

The statistics indicated that information systems security professionals employed the skills and attributes identified in Domain 2 of the CISSP, *Telecommunications and Network Security*, in an information systems security work environment. The statistical analysis of the questions representing Domain 2 indicated the null hypotheses, Ho1: The

skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, and Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, were not rejected.

### *Domain 3 Analysis*

Three questions were used to evaluate Domain 3, *Security Management Practices*. For information systems security professionals, these questions were:

1. Pro6, how often do you employ implementation and management of change control?
2. Pro7, how often do you employ the development or implementation of information security employment policies, practices, standards, guidelines, and procedures?
3. Pro8, how often do you employ security awareness training and management?

For information systems security faculty these questions were:

1. Edu6 how often do you teach implementation and management of change control?
2. Edu7, how often do you teach the development or implementation of information security employment policies, practices, standards, guidelines, and procedures?
3. Edu8, how often do you teach security awareness training and management?

The scaling of the survey was as follows: always (5), often (4), sometimes (3), rarely (2), and never (1).

According to the descriptive statistics implementation and management of change control (pro6) with a mean ( $\underline{M}$ ) of 4.000) was employed more than implementation and management of change control (edu6) with a mean ( $\underline{M}$ ) of 2.7778) was taught. The negative skewness of pro6 (-.426) showed a greater number of larger values while the positive skewness of edu6 (.401) showed a greater number of lower values. The small standard error of mean indicated the means of pro6 ( $\underline{SE} = .07449$ ) and edu6 ( $\underline{SE} = .14398$ ) were good estimators of the population mean which indicated the null hypothesis, Ho1: The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, was not rejected.

Although implementation and management of change control (pro6) was employed to a greater extent than information systems security faculty taught implementation and management of change control (edu6) the Chi-Square test showed the correlation was not statistically significant ( $\chi^2 (6, \underline{N} = 99) = 9.433 \underline{P} = .398, \underline{P} > .05$ ) which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

Kendall's tau-b analysis of the employment of implementation and management of change control (pro6) and the teaching of implementation and management of change control (edu6), ( $\underline{t} (\underline{N} = 99) = -.035, \underline{t} < .10$ ) indicated no statistically significant association which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work

environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

Although descriptive statistics indicated the means of the employment of implementation and management of change control (pro6) and the teaching of implementation and management of change control (edu6) were different, the Wilcoxon Matched-Pairs Signed-Ranks, ( $W$  ( $N = 99$ ) = -5.800,  $P = .000$ ,  $P < .05$ ) indicated the difference was not coincidental.

The development or implementation of information security employment policies, practices, standards, guidelines, and procedures (pro7) with a mean ( $M$ ) of 4.1760) were employed more than the development or implementation of information security employment policies, practices, standards, guidelines, and procedures (edu7) with a mean ( $M$ ) of 4.0303) were taught. The negative skewness of pro7 (-.265) and edu7 (-1.067) showed a greater number of larger values. The small standard error of mean indicated the means of pro7 ( $SE = .06331$ ) and edu7 ( $SE = .12878$ ) were good estimators of the population mean which indicated the null hypothesis,  $H_01$ : The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, was not rejected.

Although the development or implementation of information security employment policies, practices, standards, guidelines, and procedures (pro7) were employed to a greater extent than information systems security faculty taught the development or implementation of information security employment policies, practices, standards, guidelines, and procedures (edu7) the Chi-Square test showed the correlation was not statistically significant ( $\chi^2$  (6,  $N = 99$ ) = 8.735  $P = .365$ ,  $P > .05$ ) which indicated the null

hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

Kendall's tau-b analysis of the employment of the development or implementation of information security employment policies, practices, standards, guidelines, and procedures (pro7) and the teaching of the development or implementation of information security employment policies, practices, standards, guidelines, and procedures (edu7), ( $t$  ( $N = 99$ ) = .003,  $t < .10$ ) indicated no statistically significant association which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

The descriptive statistics indicated the means of the employment of the development or implementation of information security employment policies, practices, standards, guidelines, and procedures (pro7) and the teaching of the development or implementation of information security employment policies, practices, standards, guidelines, and procedures (edu7) were different. The Wilcoxon Matched-Pairs Signed-Ranks, ( $W$  ( $N = 99$ ) = -.628,  $P = .530$ ,  $P > .05$ ) indicated the difference may be coincidental.

According to the descriptive statistics security awareness training and management (pro8) with a mean ( $M$ ) of 3.8240) was employed less than security awareness training and management (edu8) with a mean ( $M$ ) of 3.8889) was taught. The negative skewness of pro8 (-.129) and edu8 (-1.009) showed a greater number of larger values. The small

standard error of mean indicated the means of pro8 ( $SE = .07625$ ) and edu8 ( $SE = .11566$ ) were good estimators of the population mean which indicated the null hypothesis, Ho1: The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, was not rejected.

Although security awareness training and management (pro8) was employed to a lesser extent than information systems security faculty taught security awareness training and management (edu8) the Chi-Square test showed the correlation was not statistically significant ( $\chi^2 (12, N = 99) = 6.152$ ,  $P = .908$ ,  $P > .05$ ) which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being used in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

Kendall's tau-b analysis of the employment of security awareness training and management (pro8) and the teaching of security awareness training and management (edu8), ( $t (N = 99) = .089$ ,  $t < .10$ ) indicated no statistically significant association which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being used in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

The descriptive statistics indicated the means of the employment of security awareness training and management (pro8) and the teaching of security awareness training and management (edu8) were different. The Wilcoxon Matched-Pairs Signed-Ranks, ( $W (N = 99) = -1.165$ ,  $P = .244$ ,  $P > .05$ ) indicated the difference may be coincidental.



### Domain 3 Findings

The statistics indicated that information systems security professionals employed the skills and attributes identified in Domain 3 of the CISSP, *Security Management Practices*, in an information systems security work environment. The statistical analysis of the questions representing Domain 3 confirmed the null hypotheses, Ho1: The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, and Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, were not rejected.

Of interest to this research was the positive skewness of question edu6 (.401). The frequency table of edu6 showed that although the skewness was positive it was due to the lack of responses in the often (4) scale.

**Table 4, Frequency Table for Edu6**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1.00	23	18.4	23.2	23.2
	2.00	22	17.6	22.2	45.5
	3.00	31	24.8	31.3	76.8
	5.00	23	18.4	23.2	100.0
	Total	99	79.2	100.0	
Missing	System	26	20.8		
Total		125	100.0		

### *Domain 4 Analysis*

Two questions were used to evaluate Domain 4, *Applications and Systems*

*Development Security*. For information systems security professionals these were:

1. Pro9, how often do you employ information security involving database and data warehousing, and information storage?
2. Pro10, how often do you employ information security regarding knowledge based systems and development controls?

For information systems security faculty these questions were:

1. Edu9, how often do you teach information security involving database and data warehousing, and information storage?
2. Edu10, how often do you teach information security regarding knowledge based systems and development controls?

The scaling of the survey was as follows: always (5), often (4), sometimes (3), rarely (2), and never (1).

According to the descriptive statistics information security involving database and data warehousing, and information storage (pro9) with a mean ( $\bar{M}$ ) of 4.0080 was employed more than information security involving database and data warehousing, and information storage (edu9) with a mean ( $\bar{M}$ ) of 3.6768 was taught. The negative skewness of pro9 (-.963) and edu9 (-.448) showed a greater number of larger values. The small standard error of mean indicated the means of pro9 ( $SE = .08230$ ) and edu9 ( $SE = .11998$ ) were good estimators of the population mean which indicated the null hypothesis,  $H_01$ : The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, was not rejected.

Information security involving database and data warehousing, and information storage (pro9) was employed to a greater extent than information systems security faculty taught information security involving database and data warehousing, and information storage (edu9). The Chi-Square test showed the correlation was statistically significant ( $\chi^2 (16, N = 99) = 37.058$ ,  $P = .002$ ,  $P < .05$ ) which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was rejected.

Kendall's tau-b analysis of the employment of information security involving database and data warehousing, and information storage (pro9) and the teaching of information security involving database and data warehousing, and information storage (edu9), ( $t (N = 99) = .127$ ,  $t > .10$ ) indicated a statistically weak association which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was rejected.

The descriptive statistics indicated the means of the employment of information security involving database and data warehousing, and information storage (pro9) and the teaching of information security involving database and data warehousing, and information storage (edu9) were different. The Wilcoxon Matched-Pairs Signed-Ranks, ( $W (N = 99) = -2.463$ ,  $P = .014$ ,  $P < .05$ ) indicated the difference was not coincidental.

According to the descriptive statistics information security regarding knowledge based systems and development controls (pro10) with a mean ( $M$ ) of 3.4560 were employed

more than information security regarding knowledge based systems and development controls (edu10) with a mean of ( $\underline{M}$ ) of 3.2222) were taught. The negative skewness of pro10 (-.147) showed a greater number of larger values while the positive number of edu10 (.251) showed a greater number of smaller values. The small standard error of mean indicated the means of pro10 ( $\underline{SE} = .09538$ ) and edu10 ( $\underline{SE} = .10507$ ) were good estimators of the population mean which indicated the null hypothesis, Ho1: The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, was not rejected.

Information security regarding knowledge based systems and development controls (pro10) was employed to a greater extent than information systems security faculty taught information security regarding knowledge based systems and development controls (edu10). The Chi-Square test showed the correlation was statistically significant ( $\chi^2$  (16,  $\underline{N} = 99$ ) = 22.802  $\underline{P} = .029$ ,  $\underline{P} < .05$ ) which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was rejected.

Kendall's tau-b analysis of the employment of information security regarding knowledge based systems and development controls (pro10) and the teaching of information security regarding knowledge based systems and development controls (edu10), ( $\underline{t}$  ( $\underline{N} = 99$ ) = .121,  $\underline{t} > .10$ ) indicated a statistically weak association which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work

environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was rejected.

The descriptive statistics indicated the means of the employment of information security regarding knowledge based systems and development controls (pro10) and the teaching of information security regarding knowledge based systems and development controls (edu10) were different. The Wilcoxon Matched-Pairs Signed-Ranks, ( $W(N = 99) = -2.146, P = .032, P < .05$ ) indicated the difference was not coincidental.

#### *Domain 4 Findings*

The statistics indicated that information systems security professionals employed the skills and attributes identified in Domain 4 of the CISSP, *Applications and Systems Development Security*, in an information systems security work environment and there was a correlation between what was employed and what was taught. The statistical analysis of the questions representing Domain 4 indicated the null hypothesis, Ho1: The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, was not rejected, but the null hypothesis, Ho2: There is no association between the skills and attributes identified as being used in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was rejected.

Of interest to this research was the difference in skewness of question pro10 (-.147) and edu10 (.251). A review of the frequency table (see Table 5) showed that although the skewness was almost normal it was due to the lack of responses in the often (4) scale, whereas pro6 (see Table 6) indicated the significant number of responses were in the sometimes (3), often (4) and always (5) scales.

**Table 5, Frequency Table for Edu10**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1.00	7	5.6	7.1	7.1
	2.00	4	3.2	4.0	11.1
	3.00	68	54.4	68.7	79.8
	5.00	20	16.0	20.2	100.0
	Total	99	79.2	100.0	
Missing	System	26	20.8		
	Total	125	100.0		

**Table 6, Frequency Table for Pro10**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1.00	3	2.4	2.4	2.4
	2.00	22	17.6	17.6	20.0
	3.00	39	31.2	31.2	51.2
	4.00	37	29.6	29.6	80.8
	5.00	24	19.2	19.2	100.0
	Total	125	100.0	100.0	

### *Domain 5 Analysis*

Two questions were used to evaluate Domain 5, *Cryptography*. For information systems security professionals these questions were:

1. Pro11, how often do you employ cryptographic concepts, methodologies and practices, private and public key algorithms, and public key infrastructure?

2. Pro12, how often do you employ system architecture for implementing cryptographic functions?

For information systems security faculty these questions were:

1. Edu11, how often do you teach cryptographic concepts, methodologies and practices, private and public key algorithms, and public key infrastructure?
2. Edu12, how often do you teach system architecture for implementing cryptographic functions?

The scaling of the survey was as follows: always (5), often (4), sometimes (3), rarely (2), and never (1).

According to the descriptive statistics cryptographic concepts, methodologies and practices, private and public key algorithms, and public key infrastructure (pro11) with a mean ( $\bar{M}$ ) of 3.6960 were employed less than cryptographic concepts, methodologies and practices, private and public key algorithms, and public key infrastructure (edu11) with a mean ( $\bar{M}$ ) of 4.0808 were taught. The negative skewness of pro11 (-.419) and edu11 (-1.350) showed a greater number of larger values. The small standard error of mean indicated the means of pro11 ( $\underline{SE} = .07023$ ) and edu11 ( $\underline{SE} = .13055$ ) were good estimators of the population mean which indicated the null hypothesis,  $H_0$ : The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, was not rejected.

Although cryptographic concepts, methodologies and practices, private and public key algorithms, and public key infrastructure (pro11) were employed to a greater extent than information systems security faculty taught cryptographic concepts, methodologies and practices, private and public key algorithms, and public key infrastructure (edu11) the

Chi-Square showed the correlation was not statistically significant ( $\chi^2 (16, N = 99) = 16.371$ ,  $P = .427$ ,  $P > .05$ ) which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education security curriculum, was not rejected.

Kendall's tau-b analysis of the employment of cryptographic concepts, methodologies and practices, private and public key algorithms, and public key infrastructure (pro11) and the teaching of cryptographic concepts, methodologies and practices, private and public key algorithms, and public key infrastructure (edu11), ( $t (N = 99) = -.057$ ,  $t < .10$ ) indicated no statistically significant association which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

The descriptive statistics indicated the means of the employment of cryptographic concepts, methodologies and practices, private and public key algorithms, and public key infrastructure (pro11) and the teaching of cryptographic concepts, methodologies and practices, private and public key algorithms, and public key infrastructure (edu11) were different. The Wilcoxon Matched-Pairs Signed-Ranks, ( $W (N = 99) = -2.538$ ,  $P = .011$ ,  $P < .05$ ) indicated the difference was not coincidental.

According to the descriptive statistics system architecture for implementing cryptographic functions (pro12) with a mean ( $M$ ) of 3.3200 was employed more than



system architecture for implementing cryptographic functions (edu12) with a mean (M) of 3.0505 was taught. The negative skewness of pro12 (-.377) and edu12 (-.038) showed a greater number of larger values. The small standard error of mean indicated the means of pro12 (SE = .08843) and edu12 (SE = .13031) were good estimators of the population mean which indicated the null hypothesis, Ho1: The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, was not rejected.

Although system architecture for implementing cryptographic functions (pro12) was employed to a greater extent than information systems security faculty taught system architecture for implementing cryptographic functions (edu12) the Chi-Square test showed the correlation was not statistically significant ( $\chi^2 (16, \underline{N} = 99) = 13.451$  P = .640, P > .05) which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

Kendall's tau-b analysis of the employment of system architecture for implementing cryptographic functions (pro12) and the teaching of system architecture for implementing cryptographic functions (edu12), (t (N = 99) = .039, t < .10) indicated no statistically significant association which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

The descriptive statistics indicated the means of the employment of system architecture for implementing cryptographic functions (pro12) and the teaching of system architecture for implementing cryptographic functions (edu12) were different. The Wilcoxon Matched-Pairs Signed-Ranks, ( $W$  ( $N = 99$ ) = -1.953,  $P = .051$ ,  $P > .05$ ) confirmed the difference may be coincidental.

#### *Domain 5 Findings*

The statistics indicated that information systems security professionals employed the skills and attributes identified in Domain 5 of the CISSP, *Cryptography*, in an information systems security work environment. The statistical analysis of the questions representing Domain 5 indicated the null hypotheses, Ho1: The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, and Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, were not rejected.

#### *Domain 6 Analysis*

Three questions were used to evaluate Domain 6, *Security Architecture and Models*.

For information systems security professionals these were:

1. Pro13, how often do you employ principles of common computer and network organizations, principles of common security models, and evaluation techniques?
2. Pro14, how often are you confronted with common flaws and security issues associated with systems architecture and design?
3. Pro15, how often do you employ systems architecture evaluation techniques?

For information systems security faculty these questions were:

1. Edu13, how often do you teach principles of common computer and network organizations, principles of common security models, and evaluation techniques?
2. Edu14, how often do you teach common flaws and security issues associated with systems architecture and design?
3. Edu15, how often do you teach systems architecture evaluation techniques?

The scaling of the survey was as follows: always (5), often (4), sometimes (3), rarely (2), and never (1).

According to the descriptive statistics principles of common computer and network organizations, principles of common security models, and evaluation techniques (pro13) with a mean (M) of 3.9440 were employed less than principles of common computer and network organizations, principles of common security models, and evaluation techniques (edu13) with a mean (M) of 3.9798 were taught. The negative skewness of pro13 (-.418) and edu13 (-1.190) showed a greater number of larger values. The small standard error of mean indicated the means of pro13 (SE = .07388) and edu13 (SE = .13993) were good estimators of the population which indicated the null hypothesis, Ho1: The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, was not rejected.

Although principles of common computer and network organizations, principles of common security models, and evaluation techniques (pro13) were employed to a lesser extent than information systems security faculty taught principles of common computer and network organizations, principles of common security models, and evaluation techniques (edu13) the Chi-Square test showed the correlation was not statistically

significant ( $\chi^2 (16, N = 99) = 17.137$ ,  $P = .145$ ,  $P > .05$ ) which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

Kendall's tau-b analysis of the employment of principles of common computer and network organizations, principles of common security models, and evaluation techniques (pro13) and the teaching of principles of common computer and network organizations, principles of common security models, and evaluation techniques (edu13), ( $t (N = 99) = .095$ ,  $t < .10$ ) indicated no statistically significant association which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

The descriptive statistics indicated the means of the employment of principles of common computer and network organizations, principles of common security models, and evaluation techniques (pro13) and the teaching of principles of common computer and network organizations, principles of common security models, and evaluation techniques (edu13) were different. The Wilcoxon Matched-Pairs Signed-Ranks, ( $W (N = 99) = -.576$ ,  $P = .564$ ,  $P > .05$ ) indicated the difference may be coincidental.

According to the descriptive statistics common flaws and security issues associated with systems architecture and design (pro14) with a mean ( $M$ ) of 4.1520 were confronted more than common flaws and security issues associated with systems architecture and

design (edu14) with a mean (M) of 3.9091 were taught. The negative skewness of pro14 (-.344) and edu14 (-1.106) showed a greater number of larger values. The small standard error of mean indicated the means of pro14 (SE = .05909) and edu14 (SE = .14001) were good estimators of the population mean which indicated the null hypothesis, Ho1: The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, was not rejected.

Although common flaws and security issues associated with systems architecture and design (pro14) were confronted to a greater extent than information systems security faculty taught common flaws and security issues associated with systems architecture and design (edu14) the Chi-Square test showed the correlation was not statistically significant ( $\chi^2$  (16, N = 99) = 13.126 P = .360, P > .05) which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

Kendall's tau-b analysis of the confrontation of common flaws and security issues associated with systems architecture and design (pro14) and the teaching of common flaws and security issues associated with systems architecture and design (edu14), (t (N = 99) = .063, t < .10) indicated no statistically significant association which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

The descriptive statistics indicated the means of the confrontation of common flaws and security issues associated with systems architecture and design (pro14) and the teaching of common flaws and security issues associated with systems architecture and design (edu14) were different. The Wilcoxon Matched-Pairs Signed-Ranks, ( $W$  ( $N = 99$ ) = -1.371,  $P = .170$ ,  $P > .05$ ) indicated the difference may be coincidental.

According to the descriptive statistics systems architecture evaluation techniques (pro15) with a mean ( $M$ ) of 3.5680 were employed more than systems architecture evaluation techniques (edu15) with a mean ( $M$ ) of 3.1313 were taught. The negative skewness of pro15 (-.064) and edu15 (-.060) showed a greater number of larger values. The small standard error of mean indicated the means of pro15 ( $SE = .07815$ ) and edu15 ( $SE = .11633$ ) were good estimators of the population mean which indicated the null hypothesis, Ho1: The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, was not rejected.

Although systems architecture evaluation techniques (pro15) were employed to a greater extent than information systems security faculty taught systems architecture evaluation techniques (edu15) the Chi-Square test showed the correlation was not statistically significant ( $\chi^2(16, N = 99) = 9.281$   $P = .901$ ,  $P > .05$ ) which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

Kendall's tau-b analysis of the employment of systems architecture evaluation techniques (pro15) and the teaching of systems architecture evaluation techniques

(edu15), ( $t(N = 99) = .132, t > .10$ ) indicated a statistically weak association which when compared with the other statistical tests indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

The descriptive statistics indicated the means of the employment of systems architecture evaluation techniques (pro15) and the teaching of systems architecture evaluation techniques (edu15) were different. The Wilcoxon Matched-Pairs Signed-Ranks, ( $W(N = 99) = -3.176, P = .001, P < .05$ ) indicated the difference was not coincidental.

### *Domain 6 Findings*

The statistics indicated that information systems security professionals employed the skills and attributes identified in Domain 6 of the CISSP, *Security Architecture and Models*, in an information systems security work environment. The statistical analysis of the questions representing Domain 6 indicated the null hypotheses, Ho1: The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, and Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, were not rejected.

### *Domain 7 Analysis*

Two questions were used to evaluate Domain 7, *Operations Security*. For information systems security professionals these were:

1. Pro16, how often do you employ administrative management concepts, resource protection, audit trails, inappropriate activities, violations, breaches, and reporting?
2. Pro17, how often do you employ monitoring tools and techniques, intrusion detection and penetration detection techniques, threats and counter measures?

For information systems security faculty these questions were:

1. Edu16, how often do you teach administrative management concepts, resource protection, audit trails, inappropriate activities, violations, breaches, and reporting?
2. Edu17, how often do you teach monitoring tools and techniques, intrusion detection and penetration detection techniques, threats and counter measures?

The scaling of the survey was as follows: always (5), often (4), sometimes (3), rarely (2), and never (1).

According to the descriptive statistics administrative management concepts, resource protection, audit trails, inappropriate activities, violations, breaches, and reporting (pro16) with a mean (M) of 4.1200 were employed more than administrative management concepts, resource protection, audit trails, inappropriate activities, violations, breaches, and reporting (edu16) with a mean (M) of 3.4343 were taught. The small positive skewness of pro16 (.069) showed the numbers were clustered around the middle values, while the negative skewness of edu16 (-.283) showed a greater number of



larger values. The small standard error of mean indicated the means of pro16 ( $SE = .04899$ ) and edu16 ( $SE = .13932$ ) were good estimators of the population mean which indicated the null hypothesis, Ho1: The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, was not rejected.

Although administrative management concepts, resource protection, audit trails, inappropriate activities, violations, breaches, and reporting (pro16) were employed to a greater extent than information systems security faculty taught administrative management concepts, resource protection, audit trails, inappropriate activities, violations, breaches, and reporting (edu16) the Chi-Square test showed the correlation was not statistically significant ( $\chi^2 (6, N = 99) = 5.867$   $P = .438$ ,  $P > .05$ ) which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

Kendall's tau-b analysis of the employment of administrative management concepts, resource protection, audit trails, inappropriate activities, violations, breaches, and reporting (pro16) and the teaching of administrative management concepts, resource protection, audit trails, inappropriate activities, violations, breaches, and reporting (edu16), ( $t (N = 99) = .177$ ,  $t > .10$ ) indicated a statistically weak association which, when combined with the results of the Chi-Square statistic, indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in

designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

The descriptive statistics indicated the means of the employment of administrative management concepts, resource protection, audit trails, inappropriate activities, violations, breaches, and reporting (pro16) and the teaching of administrative management concepts, resource protection, audit trails, inappropriate activities, violations, breaches, and reporting (edu16) were different. The Wilcoxon Matched-Pairs Signed-Ranks, ( $W(N = 99) = -4.367, P = .000, P < .05$ ) indicated the difference was not coincidental.

According to the descriptive statistics monitoring tools and techniques, intrusion detection and penetration detection techniques, threats and counter measures (pro17) with a mean ( $M$ ) of 4.0480 were employed more than monitoring tools and techniques, intrusion detection and penetration detection techniques, threats and counter measures (edu17) with a mean ( $M$ ) of 3.9495 were taught. The negative skewness of pro17 (-1.142) and edu17 (-.802) showed a greater number of larger values. The small standard error of mean indicated the means of pro17 ( $SE = .07776$ ) and edu17 ( $SE = .13266$ ) were good estimators of the population mean which indicated the null hypothesis,  $H_0$ : The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, was not rejected.

Although monitoring tools and techniques, intrusion detection and penetration detection techniques, threats and counter measures (pro17) were employed to a greater extent than information systems security faculty taught monitoring tools and techniques, intrusion detection and penetration detection techniques, threats and counter measures

(edu17) the Chi-Square test showed the correlation was statistically significant ( $\chi^2 (12, N = 99) = 22.077$ ,  $P = .037$ ,  $P < .05$ ) which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was rejected.

Kendall's tau-b analysis of the employment of monitoring tools and techniques, intrusion detection and penetration detection techniques, threats and counter measures (pro17) and the teaching of monitoring tools and techniques, intrusion detection and penetration detection techniques, threats and counter measures (edu17), ( $t (N = 99) = .109$ ,  $t > .10$ ) indicated a statistically weak association which, when combined with the results of the Chi-Square statistic, indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was rejected.

The descriptive statistics indicated the means of the employment of monitoring tools and techniques, intrusion detection and penetration detection techniques, threats and counter measures (pro17) and the teaching of monitoring tools and techniques, intrusion detection and penetration detection techniques, threats and counter measures (edu17) were different. The Wilcoxon Matched-Pairs Signed-Ranks, ( $W (N = 99) = -1.071$ ,  $P = .284$ ,  $P > .05$ ) indicated the difference may be coincidental.

### *Domain 7 Findings*

The statistics indicated that information systems security professionals employed the skills and attributes identified in Domain 7 of the CISSP, *Operations Security*, in an

information systems security work environment. The statistical analysis of the questions representing Domain 7 indicated the null hypotheses, Ho1: The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, and Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, were not rejected for questions pro16 and edu16. However, the statistical analysis of questions pro17 and edu17 indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was rejected.

### *Domain 8 Analysis*

Two questions were used to evaluate Domain 8, *Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)*. For information systems security professionals these were:

1. Pro18, how often do you employ protection of critical business processes?
2. Pro19, how often do you employ procedures for emergency response, extended back-up and post-disaster recovery?

For information systems security faculty these questions were:

1. Edu18, how often do you teach protection of critical business processes?
2. Edu19, how often do you teach procedures for emergency response, extended back-up and post-disaster recovery?

The scaling of the survey was as follows: always (5), often (4), sometimes (3), rarely (2), and never (1).

According to the descriptive statistics protection of critical business processes (pro18) with a mean (M) of 4.1680 was employed more than protection of critical business processes (edu18) with a mean (M) of 3.3838 was taught. The negative skewness of pro18 (-.520) and edu18 (-.221) showed a greater number of larger values. The small standard error of mean indicated the means of pro18 (SE =.06695) and edu18 (SE = .13824) were good estimators of the population mean which indicated the null hypothesis, Ho1: The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, was not rejected.

Although protection of critical business processes (pro18) was employed to a greater extent than information systems security faculty taught protection of critical business processes (edu18) the Chi-Square test showed the correlation was not statistically significant ( $\chi^2$  (9, N = 99) = 10.944 P = .280, P > .05) which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

Kendall's tau-b analysis of the employment of the protection of critical business processes (pro18) and the teaching of protection of critical business processes (edu18), (t (N = 99) = -.109, t > .10) indicated a statistically weak association, which when combined with the results of the Chi-Square statistic, indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in

an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

The descriptive statistics indicated the means of the employment of the protection of critical business processes (pro18) and the teaching of the protection of critical business processes (edu18) were different. The Wilcoxon Matched-Pairs Signed-Ranks, ( $W$  ( $N = 99$ ) = -4.220,  $P = .000$ ,  $P < .05$ ) indicated the difference was not coincidental.

According to the descriptive statistics procedures for emergency response, extended back-up and post-disaster recovery (pro19) with a mean ( $M$ ) of 3.6800 were employed more than procedures for emergency response, extended back-up and post-disaster recovery (edu19) with a mean ( $M$ ) of 3.6970 were taught. The negative skewness of pro19 (-.275) and edu19 (-.914) showed a greater number of larger values. The small standard error of mean indicated the means of pro19 ( $SE = .08546$ ) and edu19 ( $SE = .14174$ ) were good estimators of the population mean which indicated the null hypothesis, Ho1: The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, was not rejected.

Although procedures for emergency response, extended back-up and post-disaster recovery (pro19) were employed to a greater extent than information systems security faculty taught procedures for emergency response, extended back-up and post-disaster recovery (edu19) the Chi-Square test showed the correlation was not statistically significant ( $\chi^2$  (16,  $N = 99$ ) = 15.355  $P = .499$ ,  $P > .05$ ) which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being

taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

Kendall's tau-b analysis of the employment of procedures for emergency response, extended back-up and post-disaster recovery (pro19) and the teaching of procedures for emergency response, extended back-up and post-disaster recovery (edu19), ( $t(N = 99) = -.089, t < .10$ ) indicated no statistically significant association which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

The descriptive statistics indicated the means of the employment of the procedures for emergency response, extended back-up and post-disaster recovery (pro19) and the teaching of procedures for emergency response, extended back-up and post-disaster recovery (edu19) were different. The Wilcoxon Matched-Pairs Signed-Ranks, ( $W(N = 99) = -.783, P = .434, P > .05$ ) indicated the difference may be coincidental.

#### *Domain 8 Findings*

The statistics indicated that information systems security professionals employed the skills and attributes identified in Domain 8 of the CISSP, *Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)*, in an information systems security work environment. The statistical analysis of the questions representing Domain 8 indicated the null hypotheses, Ho1: The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, and Ho2: There is no association between the skills and attributes identified as being employed in an

information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, were not rejected.

### *Domain 9 Analysis*

Three questions were used to evaluate Domain 9, *Laws, Investigations and Ethics*.

For information systems security professionals these were:

1. Pro20, how often do you address the issue of computer crime?
2. Pro21, how often do you employ information security incident handling and investigations?
3. Pro22, how often do you employ the concepts of computer ethics?

For information systems security faculty these questions were:

1. Edu20, how often do you teach the issue of computer crime?
2. Edu21, how often do you teach information security incident handling and investigations?
3. Edu22, how often do you teach the concepts of computer ethics?

The scaling of the survey was as follows: always (5), often (4), sometimes (3), rarely (2), and never (1).

According to the descriptive statistics the issue of computer crime (pro20) with a mean ( $\bar{M}$ ) of 3.0320 was addressed less than the issue of computer crime (edu20) with a mean ( $\bar{M}$ ) of 4.3030 was taught. The positive skewness of pro20 (.294) showed a greater number of middle values. The negative skewness of edu20 (-1.476) showed a greater number of larger values. The small standard error of mean indicated the means of pro20 ( $SE = .07356$ ) and edu20 ( $SE = .09132$ ) were good estimators of the population mean



which indicated the null hypothesis, Ho1: The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, was not rejected.

Although the issue of computer crime (pro20) was addressed to a lesser extent than information systems security faculty taught the issue of computer crime (edu20) the Chi-Square test showed the correlation was not statistically significant ( $\chi^2 (16, N = 99) = 14.883$   $\underline{P} = .533$ ,  $\underline{P} > .05$ ) which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

Kendall's tau-b analysis of addressing the issue of computer crime (pro20) and the teaching of the issue of computer crime (edu20), ( $t (N = 99) = -.028$ ,  $t < .10$ ) indicated no statistically significant association which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

The descriptive statistics indicated the means of addressing the issue of computer crime (pro20) and teaching the issue of computer crime (edu20) were different. The Wilcoxon Matched-Pairs Signed-Ranks, ( $W (N = 99) = -7.124$ ,  $\underline{P} = .000$ ,  $\underline{P} < .05$ ) confirmed the difference was not coincidental.

According to the descriptive statistics information security incident handling and investigations (pro21) with a mean ( $\bar{M}$ ) of 3.4480 were employed slightly more than information security incident handling and investigations (edu21) with a mean ( $\bar{M}$ ) of 3.4444 were taught. The negative skewness of pro21 (-.236) and edu21 (-.562) indicated a greater number of larger values. The small standard error of mean indicated the means of pro21 ( $SE = .08832$ ) and edu21 ( $SE = .16194$ ) were good estimators of the population mean which indicated the null hypothesis, Ho1: The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, was not rejected.

Although information security incident handling and investigations (pro21) were employed to a greater extent than information systems security faculty taught information security incident handling and investigations (edu21) the Chi-Square test showed the correlation was not statistically significant ( $\chi^2 (16, N = 99) = 20.343$   $P = .205$ ,  $P > .05$ ) which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

Kendall's tau-b analysis of the employment of information security incident handling and investigations (pro21) and the teaching of information security incident handling and investigations (edu21), ( $t (N = 99) = -.057$ ,  $t < .10$ ) indicated no statistically significant association which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work

environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

The descriptive statistics indicated the means of the employment of information security incident handling and investigations (pro21) and the teaching of information security incident handling and investigations (edu21) were different. The Wilcoxon Matched-Pairs Signed-Ranks, ( $W$  ( $N = 99$ ) = -.089,  $P = .929$ ,  $P < .05$ ) indicated the difference may be coincidental.

According to the descriptive statistics concepts of computer ethics (pro22) with a mean ( $M$ ) of 3.7440 were employed slightly more than concepts of computer ethics (edu22) with a mean ( $M$ ) of 3.5556 were taught. The negative skewness of pro22 (-.227) and edu22 (-.747) showed a greater number of larger values. The small standard error of mean indicated the means of pro22 ( $SE = .08644$ ) and edu22 ( $SE = .16696$ ) were good estimators of the population mean which indicated the null hypothesis,  $H_01$ : The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, was not rejected.

Although the concepts of computer ethics (pro22) were employed to a greater extent than information systems security faculty taught the concepts of computer ethics (edu22) the Chi-Square test showed the correlation was not statistically significant ( $\chi^2$  (16,  $N = 99$ ) = 7.994  $P = .949$ ,  $P > .05$ ) which indicated the null hypothesis,  $H_02$ : There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

Kendall's tau-b analysis of the employment of the concepts of computer ethics (pro22) and the teaching of the concepts of computer ethics (edu22), ( $t(N = 99) = -.026, t < .10$ ) indicated no statistically significant association which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

The descriptive statistics indicated the means of employment of the concepts of computer ethics (pro22) and the teaching of the concepts of computer ethics (edu22) were different. The Wilcoxon Matched-Pairs Signed-Ranks, ( $W(N = 99) = -.777, P = .437, P < .05$ ) indicated the difference may be coincidental.

### *Domain 9 Findings*

The statistics indicated that information systems security professionals employed the skills and attributes identified in Domain 9 of the CISSP, *Laws, Investigations and Ethics*, in an information systems security work environment. The statistical analysis of the questions representing Domain 1 indicated the null hypotheses, Ho1: The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, and Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, were not rejected.

Of interest to this research was the difference in skewness of questions pro20 (.294) and edu20 (-1.476). As shown in Table 7, the frequencies of pro20 showed that the skewness is almost normal due to the number of responses in the sometimes (3) scale.

As shown in Table 8, information systems security faculty taught the concept of computer crime significantly more than the concept of computer crime was employed in industry.

**Table 7, Frequency Table for Pro20**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1.00	3	2.4	2.4	2.4
	2.00	24	19.2	19.2	21.6
	3.00	71	56.8	56.8	78.4
	4.00	20	16.0	16.0	94.4
	5.00	7	5.6	5.6	100.0
	Total	125	100.0	100.0	

**Table 8, Frequency Table for Edu20**

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	1.00	2	1.6	2.0	2.0
	2.00	2	1.6	2.0	4.0
	3.00	12	9.6	12.1	16.2
	4.00	31	24.8	31.3	47.5
	5.00	52	41.6	52.5	100.0
	Total	99	79.2	100.0	
Missing	System	26	20.8		

---

Total	125	100.0
-------	-----	-------

---

### *Domain 10 Analysis*

One question was used to evaluate Domain 10, *Physical Security*. For information systems security professionals this question was:

1. Pro23, how often do you employ the concepts of protection from physical security threats?

For information systems security faculty this question was:

2. Edu23, how often do you teach the concepts of protection from physical security threats?

The scaling of the survey was as follows: always (5), often (4), sometimes (3), rarely (2), and never (1).

According to the descriptive statistics concepts of protection from physical security threats (pro23) with a mean (M) of 3.9040 were employed slightly more than concepts of protection from physical security threats (edu23) with a mean (M) of 3.6768 were taught. The negative skewness of pro23 (-.058) and edu23 (-.765) showed a greater number of larger values. The small standard error of mean indicated the means of pro23 (SE = .07571) and edu23 (SE = .13908) were good estimators of the population mean which indicated the null hypothesis,  $H_0$ : The skills and attributes identified in the ten domains of the CISSP are employed in an information systems security work environment, was not rejected.

Although concepts of the employment of protection from physical security threats (pro23) were employed to a greater extent than information systems security faculty

taught concepts of protection from physical security threats (edu23) the Chi-Square test showed the correlation was not statistically significant ( $\chi^2 (16, N = 99) = 7.893$   $P = .793$ ,  $P > .05$ ) which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

Kendall's tau-b analysis of the employment of the concepts of protection from physical security threats (pro23) and the teaching of the concepts of protection from physical security threats (edu23), ( $t (N = 99) = -.045$ ,  $t < .10$ ) indicated no statistically significant association which indicated the null hypothesis, Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, was not rejected.

The descriptive statistics indicated the means of employment of the concepts of protection from physical security threats (pro23) and the teaching of the concepts of protection from physical security threats (edu23) were different. The Wilcoxon Matched-Pairs Signed-Ranks, ( $W (N = 99) = -.839$ ,  $P = .402$ ,  $P < .05$ ) indicated the difference may be coincidental.

### *Domain 10 Findings*

The statistics indicated that information systems security professionals employed the skills and attributes identified in Domain 10 of the CISSP, *Physical Security*, in an information systems security work environment. The statistical analysis of the questions representing Domain 10 indicated the null hypotheses, Ho1: The skills and attributes

identified in the ten domains of the CISSP are employed in an information systems security work environment, and Ho2: There is no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education, were not rejected.



## Chapter 5

### Conclusions, Implications, Recommendations, and Summary

#### **Conclusions**

This research examined the 10 CISSP domains to determine if the skills and attributes identified in these domains were being employed in an information systems security work environment and then examined existing NSA Centers of Academic Excellence in Information Assurance Education to determine if these skills and attributes were being taught.

Four questions were used to evaluate Domain 1, *Access Control Systems and Methodology*, covering the following skills and attributes: access control techniques, access control administration and access control models; identification and authentication techniques; intrusion detection monitoring and penetration testing; and International Standards Organization/Open Systems Interconnection, layers and characteristics. The results of comparing the skills and attributes employed with those being taught indicated that the skills and attributes in Domain 1 were being employed by information systems security professionals in an information systems security work environment and there was no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education.

One question was used to evaluate Domain 2, *Telecommunications and Network Security*, covering the following skills and attributes: security controls when addressing communications and network security, Internet/Intranet/Extranet, e-mail security, facsimile security, secure voice communications, and security boundaries. The results of comparing the skills and attributes employed with those being taught indicated that the skills and attributes in Domain 2 were being used by information systems security professionals in an information systems security work environment and there was no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education.

Three questions were used to evaluate Domain 3, *Security Management Practices*, covering the following skills and attributes: implementation and management of change control; the development or implementation of information systems security employment policies, practices, standards, guidelines, and procedures; and security awareness training and management. The results of comparing the skills and attributes employed with those being taught indicated that the skills and attributes in Domain 3 were being employed by information systems security professionals in an information systems security work environment and there was no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education.

Domain 4 was the only domain that confirmed a correlation between skills and attributes used in an information systems security work environment and those being

taught. Two questions were used to evaluate Domain 4, *Applications and Systems Development Security*, covering the following skills and attributes: information security involving database and data warehousing, and information storage; and information systems security regarding knowledge based systems and development controls. The results of comparing the skills and attributes employed with those being taught indicated that the skills and attributes in Domain 4 were being employed by information systems security professionals in an information systems security work environment and there was a statistically significant association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education.

Two questions were used to evaluate Domain 5, *Cryptography*, covering the following skills and attributes: cryptographic concepts, methodologies and practices, private and public key algorithms, and public key infrastructure; and system architecture for implementing cryptographic functions. The results of comparing the skills and attributes employed with those being taught indicated that the skills and attributes in Domain 5 were being employed by information systems security professionals in an information systems security work environment and there was no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education.

Three questions were used to evaluate Domain 6, *Security Architecture and Models*, covering the following skills and attributes: principles of common computer and network

organizations, principles of common security models, and evaluation techniques; common flaws and security issues associated with systems architecture and design; and systems architecture evaluation techniques. The results of comparing the skills and attributes employed with those being taught indicated that the skills and attributes in Domain 6 were being employed by information systems security professionals in an information systems security work environment and there was no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education.

Two questions were used to evaluate Domain 7, *Operations Security*, covering the following skills and attributes: administrative management concepts, resource protection, audit trails, inappropriate activities, violations, breaches, and reporting; and monitoring tools and techniques, intrusion detection and penetration detection techniques, threats and counter measures. The results of comparing the skills and attributes employed with those being taught indicated that the skills and attributes in Domain 7 were being employed by information systems security professionals in an information systems security work environment and there was no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education.

Two questions were used to evaluate Domain 8, *Business Continuity Planning (BCP) and Disaster Recovery Planning (DRP)* which cover the following skills and attributes: protection of critical business processes, and procedures for emergency response

extended back-up and post-disaster recovery. The results of comparing the skills and attributes employed with those being taught indicated that the skills and attributes in Domain 8 were being employed by information systems security professionals in an information systems security work environment and there was no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education.

Three questions were used to evaluate Domain 9, *Laws, Investigations and Ethics*, which cover the following skills and attributes: the issue of computer crime; information systems security incident handling and investigations; and the concepts of computer ethics. The results of comparing the skills and attributes employed with those being taught indicated that the skills and attributes in Domain 9 were being employed by information systems security professionals in an information systems security work environment and there was no association between the skills and attributes identified as being employed in an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education.

One question was used to evaluate Domain 10, *Physical Security* covering the following skills and attributes: the concepts of protection from physical security threats. The results of comparing the skills and attributes employed with those being taught indicated that the skills and attributes in Domain 10 were being employed by information systems security professionals in an information systems security work environment and there was no association between the skills and attributes identified as being employed in

an information systems security work environment and those being taught in designated NSA Centers of Academic Excellence in Information Assurance Education.

### **Implications**

A search of existing literature supported the need for a standard curriculum in information systems security. Bishop (2000), in particular, identified this need in his presentation to the National Colloquium on Information Systems Security where he defined information systems security as it applied to academia and stated the goal of undergraduate, graduate, and doctorate education was to “learn broad principles, and see how to apply them” (Bishop, 2000). This dissertation is a start at identifying and addressing the skills and attributes needed in an information systems security curriculum. The outcomes indicate that academia continues to ignore the need for teaching the broad principles of information systems security as identified by professionals in the field. These principles, as identified by the skills and attributes being employed in an information systems security work environment, are not, with one exception, taught in NSA Centers of Academic Excellence in Information Assurance Education. The one domain that is the exception is Domain 4, *Applications and Systems Development Security*, covering the following skills and attributes: information systems security involving database and data warehousing, and information storage and information systems security regarding knowledge based systems and development controls. This research confirmed a correlation, in this one area, between skills and attributes employed in an information systems security work

environment and those being taught in NSA Centers of Academic Excellence in Information Assurance Education.

### **Recommendations**

The following areas are targets for further research. Faculty and curriculum developers should review the principles of information systems security, as performed by professionals in an information systems security work environment, for incorporation into the development of information systems security curriculum and programs. NSA should add to its criteria for the designation of Centers of Academic Excellence in Information Assurance Education, the teaching of skills and attributes of information systems security as identified by these professionals.

Regarding the skills and attributes best identified as being employed in an information systems security work environment, the following three questions are indicated for further research:

- 1) What, if any, are the differences in the skills and attributes identified in the various information systems security certifications?
- 2) Is there a correlation between the skills and attributes identified in each of the information systems security certifications?
- 3) What, if any, are the differences in the employment of these skills and attributes between certified and non-certified information systems security professionals?

Regarding the skills and attributes best identified as being necessary in an information systems security curriculum, the following two questions are indicated for further research:

1. How should existing information systems security curriculum be changed to better meet the needs of information systems security professionals working in the field?
2. Should broad principles or specific applications relating to the skills and attributes identified in an information systems security work environment be taught?

Regarding the skills and attributes best identified as being taught in an information systems security curriculum, the following two questions are indicated for further research:

1. Are the skills and attributes identified in other information systems security certifications used in an information systems security work environment?
2. Are universities with information systems security curriculum teaching these skills?

## **Summary**

Although professional certifications in information systems security are based on a common body of knowledge, there is still a fundamental difference of opinion as to what constitutes this common body of knowledge. Many practitioners of information systems security feel that to further define information systems security and to legitimize its existence there should be accredited college curriculum (Saita, 2002). Information systems security as a field has not matured sufficiently to develop processes associated



with performing specific information systems security job tasks. Until these tasks are identified and related job standards produced, effective standardized information systems security curriculum can not be developed (Reynolds, 1998).

NSA identified 37 universities as meeting the standards required for recognition as Centers of Academic Excellence in Information Assurance Education. One of the standards for compliance stipulated that schools must have curriculum mapped to *National Security Telecommunications and Information Systems Security Committee (NSTISSC) 4011 National Training Standard for Information Systems Security (INFOSEC) Professionals*, an eight year old document (Centers of Academic Excellence in Information Assurance Education, 2002). The NSTISSC focus was to provide standards for practical vocational skills. Mainstream colleges and universities have goals that may or may not be compatible with those of the standards dictated by NSTISSC (Yasinsac, 1999). The Security Certification Consortium (ISC)<sup>2</sup> was instrumental in the development of the Certified Information Systems Security Professional (CISSP), the most comprehensive certification for information systems security professionals (Dugan & Prencipe, 2001). Although CISSP was not the only certification available for information systems security professionals it was the only broad top-down certification covering theoretical knowledge of ten domains recognized to be required for information systems security certification and for many organizations the CISSP was considered to be the gold standard in information systems security.

This research examined the 10 CISSP domains from within the information systems security work environment to determine which skills were necessary and then examined

existing NSA Centers of Academic Excellence in Information Assurance Education to determine which skills and attributes from within the 10 domains were being taught.

Using empirical methods the goal of this research was to determine if existing curriculum in colleges and universities designated as NSA Centers of Academic Excellence in Information Assurance Education was consistent with the needs of an information systems security work environment.

The skills and attributes within the 10 Domains of the CISSP were represented by 24 questions, one of which was identified by the validity process as being unnecessary. The breakdown of the domain descriptions into questions was accomplished during the pilot study phase. Using "The CISSP Prep Guide" ( Krutz, 2001) and the CISSP descriptions, the pilot study committee identified the sentences that best fit the skills and attributes of that domain. These sentences were converted to questions. The validity of these questions in addressing the skills and attributes was confirmed in the validity phase. The data used in this descriptive study was collected through a researcher developed survey. The survey method of data collection was chosen over the interview method due to geographic distribution of the population. The following procedures were used to develop the survey instrument: 1) develop the conceptual framework, 2) develop the operational definitions, 3) select the scaling technique, 4) review of items, 5) develop response format, 6) develop directions, 7) prepare draft and distribute pilot, 8) analyze pilot data and revise instrument (if required), 9) produce instrument, 10) conduct reliability and validity analysis, and 11) distribute survey.

From the sample of 4700 (N) information systems security professionals a random sample of 800 (n) was drawn. There were 165 invalid e-mail addresses identified.

Subtracting the invalid e-mail addresses provided a usable sample of 635. There was a non-response response rate of 80%. The non-respondents did not differ from the respondents with regard to important characteristics. The statistical analyses had taken into account both the sampling design, and the response probabilities.

For information systems security faculty a sample of 321 (N) the total 321 (n) was used. There were 20 invalid e-mail addresses identified. Subtracting the invalid e-mail addresses provided a usable sample of 301. There was a non-response rate of 67%. The non-respondents did not differ from the respondents with regard to important characteristics. The statistical analyses had taken into account both the sampling design, and the response probabilities.

This research indicated that information systems security professionals working in an information systems security work environment employed or addressed the skills and attributes identified in the 10 domains of the CISSP. This research also indicated that the skills and attributes taught in the curriculum of NSA Centers of Academic Excellence in Information Assurance Education had no association with the skills and attributes employed, or addressed, by information systems security professionals with the exception of Domain 4. There were two questions used to evaluate Domain 4, covering the following skills and attributes: information systems security involving database and data warehousing, and information storage; and information systems security regarding knowledge based systems and development controls. This research indicated that the skills and attributes identified in Domain 4 were used in an information systems security work environment and there was an association between what was being employed and what was being taught.

It should be emphasized that this research was designed to evaluate the skills and attributes relating to the CISSP certification and existing curriculum in institutions designated as Centers of Academic Excellence in Information Assurance Education. It did not look at any of the many ongoing information systems security programs at schools not so recognized by NSA, nor did it consider any of the skills and attributes identified by any of the other information systems security certifications available. As such, the results from this research should be kept in the context of an evaluation of the skills and attributes identified only in the CISSP and confined to the curriculum in NSA designated Centers of Academic Excellence in Information Assurance Education.

## Appendix A

### Pilot Survey Committee Members

Name	Position/Experience
Gene M. Gordon, Ph.D.	Associate Professor and Chair Computer and Information Systems (25 years experience)
Carl J. Chimi, Ph.D.	Associate Professor, Computer and Information Systems (23 years experience)
Charles J. Hoppel, Ph.D.	Associate Professor, Computer and Information Systems (30 years experience)
István Molnár, Ph.D.	Associate Professor, Computer and Information Systems (10 years experience)
A. Rao Korukonda, Ph.D.	Professor, Computer and Information Systems (20 years experience)
Loreen Butcher-Powell, M.S.	Assistant Professor, Business Education and Office Information Systems (4 years experience)

## Appendix B

### Pilot Survey Cover Letter

«FirstName» «LastName», «Title»  
«Rank»  
Bloomsburg University  
Bloomsburg, PA 17815

«Date»

Dear «FirstName»:

As a member of the information systems faculty at Bloomsburg University your expert advice is needed to pilot test the attached survey. This survey will be used to compare the tasks performed by information security professionals in the field with the skills being taught in information security curriculum. At this time I am not interested in your responses to the survey itself, only in the evaluation of the survey format, language, and completion time. Any comments you have will be welcome.

After completing the survey please go to <http://cob.bloomu.edu/afundaburk/pilot> to complete the evaluation form. At this web site you will be asked to evaluate the survey in terms of: 1) Are there any typographical errors? 2) Are there any misspelled words? 3) Do the numbers make sense? 4) Is the type size big enough to easily read? 5) Is the vocabulary appropriate for the respondents? 6) Is the survey too long? 7) Is the style of the items too monotonous? 8) Does the survey format flow well? 9) Are the items appropriate for the respondents? 10) Are the items sensitive to possible cultural barriers? and 11) Is the survey in the best language for the respondents?

Of further interest to this research will be the questions: 1) Does the survey adequately address the skills in an information security environment? 2) Are there any skills that should be added? and 3) Is the survey complete?

Your prompt action in evaluating this survey by August 29, 2003 will be greatly appreciated. Thank you for your willingness to participate in this research.

Web site: <http://cob.bloomu.edu/afundaburk/pilot>  
User name: evaluator

The password is: pilottester

Your PIN is: «PIN»

Al Fundaburk

Assistant Professor

Business Education/Office Information Systems

Bloomsburg University

Bloomsburg, PA 17815

## Appendix C

### Pilot Survey

#### **Information Systems Security Survey**

Start Time (                                    )

The following questions are about information security skills you might need in a typical week. How often do you perform the following skills while working in an information security environment? Please select one answer from the three categories.

1. How often, in a week, do you perform access control techniques, access control administration, and access control models?	All the time  [ ]	Sometimes  [ ]	Never  [ ]
2. How often, in a week, do you perform identification and authentication techniques?	All the time  [ ]	Sometimes  [ ]	Never  [ ]
3. How often, in a week, do you perform intrusion detection monitoring, and penetration testing?	All the time  [ ]	Sometimes  [ ]	Never  [ ]
4. How often, in a week, do you perform International Standards Organization/Open Systems Interconnection, Layers and characteristics?	All the time  [ ]	Sometimes  [ ]	Never  [ ]
5. How often, in a week, do you perform communications and network security, Internet/Intranet/Extranet, e-mail security, facsimile security, secure voice communications, and security boundaries?	All the time  [ ]	Sometimes  [ ]	Never  [ ]



6. How often, in a week, do you perform implementation and management of change control?	All the time []	Sometimes []	Never []
7. How often in a week do you perform the development or implementation of information security employment policies, practices, standards, guidelines, and procedures?	All the time []	Sometimes []	Never []
8. How often, in a week, do you perform security awareness training and management	All the time []	Sometimes []	Never []
9. How often, in a week, do you perform information security involving database and data warehousing, and information storage	All the time []	Sometimes []	Never []
10. How often, in a week do you perform information security regarding knowledge based systems and development controls	All the time []	Sometimes []	Never []
11. How often, in a week, do you perform cryptographic concepts, methodologies and practices, private and public key algorithms, and public key infrastructure	All the time []	Sometimes []	Never []
12. How often, in a week, do you perform system architecture for implementing cryptographic functions	All the time []	Sometimes []	Never []
13. How often, in a week, do you perform principles of common computer and network organizations, principles of common security models, and evaluation techniques	All the time []	Sometimes []	Never []

14. How often, in a week, do you perform common flaws and security issues associated with systems architecture and design	All the time [ ]	Sometimes [ ]	Never [ ]
15. How often, in a week, do you perform systems architecture evaluation techniques	All the time [ ]	Sometimes [ ]	Never [ ]
16. How often, in a week do you perform administrative management concepts, resource protection, audit trails, inappropriate activities, violations, breaches, and reporting	All the time [ ]	Sometimes [ ]	Never [ ]
17. How often, in a week do you perform monitoring tools and techniques intrusion detection and penetration detection techniques, threats and counter measures	All the time [ ]	Sometimes [ ]	Never [ ]
18. How often, in a week, do you perform protection of critical business processes and the effects of major failures?	All the time [ ]	Sometimes [ ]	Never [ ]
19. How often, in a week, do you use Procedures for emergency response, extended back-up and post-disaster recovery?	All the time [ ]	Sometimes [ ]	Never [ ]
20. How often, in a week, do you use Major categories and types of laws and computer crime?	All the time [ ]	Sometimes [ ]	Never [ ]
21. How often, in a week, are you involved in incident handling, and investigations?	All the time [ ]	Sometimes [ ]	Never [ ]
22. How often, in a week, do you use Computer Ethics?	All the time [ ]	Sometimes [ ]	Never [ ]
23. How often, in a week, do you use facility requirements, environment and life safety?	All the time [ ]	Sometimes [ ]	Never [ ]



## Appendix D

### Pilot Survey Evaluation Procedures

**Please list PIN here:** \_\_\_\_\_

**Now that you have completed the survey please take the time to answer these questions:**

**How long did it take you to complete the survey?** \_\_\_\_\_

- |   |         |        |
|---|---------|--------|
| <p><b>1. Are there any typographical errors?</b><br/>If yes, please describe.</p>               | Yes ( ) | No ( ) |
| <p><b>2. Are there any misspelled words?</b><br/>If yes, please describe.</p>                   | Yes ( ) | No ( ) |
| <p><b>3. Does the numbering make sense?</b><br/>If no, please describe.</p>                     | Yes ( ) | No ( ) |
| <p><b>4. Is the type size big enough to easily read?</b><br/>If no, please describe.</p>        | Yes ( ) | No ( ) |
| <p><b>5. Is the vocabulary appropriate for the respondents?</b><br/>If no, please describe.</p> | Yes ( ) | No ( ) |

6. **Is the survey too long?** Yes ( ) No ( )  
If yes, please describe.
7. **Is the style of the items too monotonous?** Yes ( ) No ( )  
If yes, please describe.
8. **Does the survey format flow well?** Yes ( ) No ( )  
If no, please describe.
9. **Are the items appropriate for the respondents?** Yes ( ) No ( )  
If no, please describe.
10. **Are the items sensitive to possible cultural barriers?** Yes ( ) No ( )  
If no, please describe.
11. **Is the survey in the best language for the respondents?** Yes ( ) No ( )  
If no, please describe.
12. **Does the survey adequately address the skills in an information security environment?** Yes ( ) No ( )  
If no, please describe.
13. **Are there any skills that should be added?** Yes ( ) No ( )  
If yes, please describe.
14. **Is the survey complete?** Yes ( ) No ( )  
If no, please describe.

Thank you for your time.

## Appendix E

### Pilot Survey Comments and Responses

---

#### Comments

---

1. You need a space after question 19; the capital P and M should be changed.  
Response: Changed.
2. You need at least five anchor responses for variability  
Response: Changed the anchors from: *All the time, Some of time, and Never to Always, Often, Sometimes, Rarely, and Never.*
3. I question the word "perform" and "USE" on some of the questions. Perhaps evaluate or apply i/o perform?  
Response: Substituted the word employ for apply and use.
4. 'The "in a week" is not needed. This was stated in the directions.  
Response: Removed the term *in a week.*
5. Additional line between Q.6 and Q.7. A line is missing between Q.19 and Q.20.  
Response: Rewritten
6. How do you perform Information security? Could this read :*How do you perform security measures?* Also some of the questions contain multiple answers. How are you accounting for this? I am not sure about the wording of question 12 and 13?  
Response: See item three. Discussed the comment on multiple answers and the wording on questions 12 and 13. Upon understanding the population and requirements and reviewing the changes this panel member had no further comments.

All changes were reviewed by the panel members and accepted.

---

## Appendix F

## Face Validity Committee Members

---

Name	Position/Experience
John J. Olivo, Ph.D.	Professor and Chair, Business Education and Office Information Systems (20 years experience)
Loreen Butcher-Powell, M.S.	Assistant Professor, Business Education and Office Information Systems (4 years experience)
Dennis O. Gehris, Ed.D.	Professor, Business Education and Office Information Systems (28 years experience)
Janice C. Keil, Ed.D.	Associate Professor, Business Education and Office Information Systems (20 years experience)
Lila D. Waldman, Ed.D.	Associate Professor, Business Education and Office Information Systems (10 years experience)

---

## Appendix G

### Validity E-mail Round One

Subject: University Info Sec Research

Dear Colleague:

As an information security professional, I am asking for your assistance in validating the content of a survey which will be used to compare the tasks performed by information security professionals in the field with the skills being taught in the information security curriculum in schools designated as National Security Agency (NSA) Centers of Excellence in Information Assurance.

As a member of this content validity panel you were chosen for your expertise and experience in the field of information security and your CISSP certification. Participation in this validation process is totally voluntary and should take no longer than 10 minutes of your time. After validation, the survey will be used as part of a dissertation titled: *The Education of Information Security Professionals: An Analysis of Industry Needs vs. Academic Curriculum in the 21<sup>st</sup> Century*. I, as the principal researcher, will be the only person viewing the collected data and to ensure anonymity all links to PINs will be deleted at the conclusion of data collection.

The purpose of the survey is to collect data to be used to classify the application of skills and attributes that are used in an information security work environment identified in the ten domains of the CISSP. These questions use a five point Likert scale for the response as follows: Always, Often, Sometimes, Rarely, and Never. As a CISSP professional you are asked to fill out a questionnaire about applicability of each of the 24 questions contained in the survey. The following rating scale is provided:

- 3 = the question correctly identifies the need
- 2 = the question is incorrectly stated; needs revision
- 1 = do not use; competency inappropriate

Please log on to <http://cob.bloomu.edu/afundaburk/content> to participate in this process.

Username: panel

Password: validate



PIN: <PIN>

I appreciate your willingness to act as a panel member in this needed research. If you have any questions, please contact me.

Al Fundaburk  
Assistant Professor  
Business Education/Office Information Systems  
Bloomsburg University  
Bloomsburg, PA 17815  
(570) 389-4816

## Appendix H

### Validity Survey Round One

**Dissertation Research Project:** *The Education of Information Security Professionals: An Analysis of Industry Needs vs. Academic Curriculum in the 21<sup>st</sup> Century*

**Principal Researcher:**

Al Fundaburk

Assistant Professor

Business Education/Office Information Systems

Bloomsburg University

(570) 389-9621

Email: [afundabr@bloomu.edu](mailto:afundabr@bloomu.edu)

Thank you for agreeing to participate in this much needed research.

The results of this study will contribute significantly to the development of extensive information security curriculum and add to the knowledge base concerning the real-world needs of information security professionals. Data will be obtained concerning: a) the knowledge and skill attributes of security professionals; and b) the effectiveness of existing curriculum.

The survey of security professionals and faculty will focus on the following domains: Access Control Systems and Methodology; Telecommunications and Network Security; Security Management Practices; Applications & Systems Development Security; Cryptography; Security Architecture; Operations Security; Business Continuity Planning & Disaster Recovery Planning; Law, Investigations & Ethics; and Physical Security.

Continue

The following questions will provide background information of respondents. The assignment of the PIN allows for individual and institutional anonymity. The participant database and survey responses will be kept confidential by the principal researcher. After survey completion, the database linking PINs to participants will be deleted--assuring participant anonymity.

Please select all that apply:

I have published textbook(s) or article(s) in the area of information security.

I have participated in at least one national or state convention as a speaker or panel member discussing the topic of information security.

I am a member of the faculty of an accredited university with a viable information security curriculum

I hold a CISSP certification

[Click here if none of the above applies to you,](#)

Otherwise please input PIN here \_\_\_\_\_ and click on submit.

The purpose of this survey is to validate the survey for the collection data to be used to classify the application of the skills and attributes identified in the ten domains of the CISSP that are used in an information security work environment. As a participant you will be asked to evaluate this survey about the use of specific information security skills. This survey is being conducted as part of a dissertation titled: *The Education of Information Security Professionals: An Analysis of Industry Needs vs. Academic Curriculum in the 21<sup>st</sup> Century*. The principal researcher is the only person viewing the collected data and all links to PINs will be deleted at the conclusion of data collection. Participation in this survey is totally voluntary and should take no longer than 10 minutes.

The following questions are about information security skills. Panel members are requested to respond to each survey question in terms of its suitability in an information security environment. The following rating scale is provided: 1) the question correctly identifies the need, 2) the question is incorrectly stated; needs revision, or 3) do not use; competency inappropriate.

### Question 1 of 24

**Please respond in terms of this question's suitability in an information security environment.**

**How often do you employ access control techniques, access control administration, and access control models?**

The question correctly identifies the need (no comment needed)

0

The question is incorrectly stated; needs revision (please comment)

0

Do not use; competency inappropriate (please comment)

0

Comments:

**Question 2 of 24**

**Please respond in terms of this question's suitability in an information security environment.**

**How often do you employ identification and authentication techniques?**

The question correctly identifies the need (no comment needed)

0

The question is incorrectly stated; needs revision (please comment)

0

Do not use; competency inappropriate (please comment)

0

Comments:

**Question 3 of 24**

**Please respond in terms of this question's suitability in an information security environment.**

**How often do you employ intrusion detection monitoring and penetration testing?**

The question correctly identifies the need (no comment needed)

0

The question is incorrectly stated; needs revision (please comment)

0

Do not use; competency inappropriate (please comment)

0

Comments:

**Question 4 of 24**

**Please respond in terms of this question's suitability in an information security environment.**

**How often do you employ International Standards Organization/Open Systems Interconnection, Layers and characteristics?**

The question correctly identifies the need (no comment needed)

0

The question is incorrectly stated; needs revision (please comment)

0

Do not use; competency inappropriate (please comment)

0

Comments:

**Question 5 of 24**

**Please respond in terms of this question's suitability in an information security environment.**

**How often do you employ communications and network security, Internet/Intranet/Extranet, e-mail security, facsimile security, secure voice communications, and security boundaries?**

The question correctly identifies the need (no comment needed)

0

The question is incorrectly stated; needs revision (please comment)

0

Do not use; competency inappropriate (please comment)

0

Comments:

**Question 6 of 24**

**Please respond in terms of this question's suitability in an information security environment.**

**How often do you employ implementation and management of change control?**

The question correctly identifies the need (no comment needed)

0

The question is incorrectly stated; needs revision (please comment)

0

Do not use; competency inappropriate (please comment)

0

Comments:

**Question 7 of 24**

**Please respond in terms of this question's suitability in an information security environment.**

**How often do you employ the development or implementation of information security employment policies, practices, standards, guidelines, and procedures?**

The question correctly identifies the need (no comment needed)

0

The question is incorrectly stated; needs revision (please comment)

0

Do not use; competency inappropriate (please comment)

0

Comments:

**Question 8 of 24**

Please respond in terms of this question's suitability in an information security environment.

**How often do you employ security awareness training and management?**

The question correctly identifies the need (no comment needed)

0

The question is incorrectly stated; needs revision (please comment)

0

Do not use; competency inappropriate (please comment)

0

Comments:

**Question 9 of 24**

Please respond in terms of this question's suitability in an information security environment.

**How often do you employ information security involving database and data warehousing, and information storage?**

The question correctly identifies the need (no comment needed)

0

The question is incorrectly stated; needs revision (please comment)

0

Do not use; competency inappropriate (please comment)

0

Comments:

**Question 10 of 24**

Please respond in terms of this question's suitability in an information security environment.

**How often do you employ information security regarding knowledge based systems and development controls?**

The question correctly identifies the need (no comment needed)

0

The question is incorrectly stated; needs revision (please comment)

0

Do not use; competency inappropriate (please comment)

0

Comments:

**Question 11 of 24**

**Please respond in terms of this question's suitability in an information security environment.**

**How often do you employ cryptographic concepts, methodologies and practices, private and public key algorithms, and public key infrastructure?**

The question correctly identifies the need (no comment needed)

0

The question is incorrectly stated; needs revision (please comment)

0

Do not use; competency inappropriate (please comment)

0

Comments:

**Question 12 of 24**

**Please respond in terms of this question's suitability in an information security environment.**

**How often do you employ system architecture for implementing cryptographic functions?**

The question correctly identifies the need (no comment needed)

0

The question is incorrectly stated; needs revision (please comment)

0

Do not use; competency inappropriate (please comment)

0

Comments:

**Question 13 of 24**

**Please respond in terms of this question's suitability in an information security environment.**

**How often do you employ principles of common computer and network organizations, principles of common security models, and evaluation techniques?**

The question correctly identifies the need (no comment needed)

0

The question is incorrectly stated; needs revision (please comment)

0

Do not use; competency inappropriate (please comment)

0

Comments:

**Question 14 of 24**

Please respond in terms of this question's suitability in an information security environment.

**How often do you employ common flaws and security issues associated with systems architecture and design?**

The question correctly identifies the need (no comment needed)

0

The question is incorrectly stated; needs revision (please comment)

0

Do not use; competency inappropriate (please comment)

0

Comments:

**Question 15 of 24**

Please respond in terms of this question's suitability in an information security environment.

**How often do you employ systems architecture evaluation techniques?**

The question correctly identifies the need (no comment needed)

0

The question is incorrectly stated; needs revision (please comment)

0

Do not use; competency inappropriate (please comment)

0

Comments:

**Question 16 of 24**

Please respond in terms of this question's suitability in an information security environment.

**How often do you employ administrative management concepts, resource protection, audit trails, inappropriate activities, violations, breaches, and reporting?**

The question correctly identifies the need (no comment needed)

0

The question is incorrectly stated; needs revision (please comment)

0

Do not use; competency inappropriate (please comment)

0

Comments:



**Question 17 of 24**

**Please respond in terms of this question's suitability in an information security environment.**

**How often do you employ monitoring tools and techniques, intrusion detection and penetration detection techniques, threats and counter measures?**

The question correctly identifies the need (no comment needed)

0

The question is incorrectly stated; needs revision (please comment)

0

Do not use; competency inappropriate (please comment)

0

Comments:

**Question 18 of 24**

**Please respond in terms of this question's suitability in an information security environment.**

**How often do you employ protection of critical business processes?**

The question correctly identifies the need (no comment needed)

0

The question is incorrectly stated; needs revision (please comment)

0

Do not use; competency inappropriate (please comment)

0

Comments:

**Question 19 of 24**

**Please respond in terms of this question's suitability in an information security environment.**

**How often do you employ procedures for emergency response, extended back-up and post-disaster recovery?**

The question correctly identifies the need (no comment needed)

0

The question is incorrectly stated; needs revision (please comment)

0

Do not use; competency inappropriate (please comment)

0

Comments:

**Question 20 of 24**

**Please respond in terms of this question's suitability in an information security environment.**

**How often do you employ the aspects of computer crime?**

The question correctly identifies the need (no comment needed)

0

The question is incorrectly stated; needs revision (please comment)

0

Do not use; competency inappropriate (please comment)

0

Comments:

**Question 21 of 24**

**Please respond in terms of this question's suitability in an information security environment.**

**How often do you employ information security incident handling and investigations?**

The question correctly identifies the need (no comment needed)

0

The question is incorrectly stated; needs revision (please comment)

0

Do not use; competency inappropriate (please comment)

0

Comments:

**Question 22 of 24**

**Please respond in terms of this question's suitability in an information security environment.**

**How often do you employ the concepts of computer ethics?**

The question correctly identifies the need (no comment needed)

0

The question is incorrectly stated; needs revision (please comment)

0

Do not use; competency inappropriate (please comment)

0

Comments:

**Question 23 of 24**

**Please respond in terms of this question's suitability in an information security environment.**

**How often do you employ the concepts of facility security requirements, environment, and life safety?**

The question correctly identifies the need (no comment needed)

0

The question is incorrectly stated; needs revision (please comment)

0

Do not use; competency inappropriate (please comment)

0

Comments:

**Question 24 of 24**

**Please respond in terms of this question's suitability in an information security environment.**

**How often do you employ the concepts of protection from physical security threats?**

The question correctly identifies the need (no comment needed)

0

The question is incorrectly stated; needs revision (please comment)

0

Do not use; competency inappropriate (please comment)

0

Comments:

## Appendix I

### Validity Results Round One

**1. How often do you employ access control techniques, access control administration, and access control models?**

Correctly Identified	Needs Revision	Inappropriate	Mean	Standard Deviation	Standard Error	95% Confidence Interval
100%	N/A	N/A	N/A	N/A	N/A	N/A

**2. How often do you employ identification and authentication techniques?**

Correctly Identified	Needs Revision	Inappropriate	Mean	Standard Deviation	Standard Error	95% Confidence Interval
94.44%	5.56%	0%	.2944	.2357	.0556	2.827 – 3.062

**3. How often do you employ intrusion detection monitoring and penetration testing?**

Correctly Identified	Needs Revision	Inappropriate	Mean	Standard Deviation	Standard Error	95% Confidence Interval
89%	11%	0%	2.889	.3234	.0762	2.728 – 3.050

**4. How often do you employ International Standards Organization/Open Systems Interconnection, Layers and characteristics?**

Correctly Identified	Needs Revision	Inappropriate	Mean	Standard Deviation	Standard Error	95% Confidence Interval
90%	5%	5%	2.778	.5438	.1292	2.505 – 3.050

**5. How often have you employed security controls when addressing communications and network security, Internet/Intranet/Extranet, e-mail security, facsimile security, secure voice communications, and security boundaries?**

Correctly Identified	Needs Revision	Inappropriate	Mean	Standard Deviation	Standard Error	95% Confidence Interval
56%	39%	6%	2.500	.6183	.1457	2.193 – 2.807

This question was revised and submitted in round 2

**6. How often do you employ implementation and management of change control?**

Correctly Identified	Needs Revision	Inappropriate	Mean	Standard Deviation	Standard Error	95% Confidence Interval
94%	6%	0%	2.889	.4714	.1111	2.654 – 3.123

**7. How often do you employ the development or implementation of information security employment policies, practices, standards, guidelines, and procedures?**

Correctly Identified	Needs Revision	Inappropriate	Mean	Standard Deviation	Standard Error	95% Confidence Interval
83%	16%	0%	2.833	.3835	.0904	2.643 – 3.024

**8. How often do you employ security awareness training and management?**

Correctly Identified	Needs Revision	Inappropriate	Mean	Standard Deviation	Standard Error	95% Confidence Interval
88%	12%	0%	2.889	.3234	.0762	2.728 – 3.305

**9. How often do you employ information security involving database and data warehousing, and information storage?**

Correctly Identified	Needs Revision	Inappropriate	Mean	Standard Deviation	Standard Error	95% Confidence Interval
94%	6%	0%	2.944	.2357	.0556	2.827 – 3.062

**10. How often do you employ information security regarding knowledge based systems and development controls?**

Correctly Identified	Needs Revision	Inappropriate	Mean	Standard Deviation	Standard Error	95% Confidence Interval

94%	6%	0%	2.944	.2357	.0556	Interval 2.827 – 3.062
-----	----	----	-------	-------	-------	------------------------------

**11. How often do you employ cryptographic concepts, methodologies and practices, private and public key algorithms, and public key infrastructure?**

Correctly Identified	Needs Revision	Inappropriate	Mean	Standard Deviation	Standard Error	95% Confidence Interval
94%	0%	6%	2.889	.4714	.1111	2.654 – 3.123

The researcher assumes the inappropriate response to be a flyer.

**12. How often do you employ system architecture for implementing cryptographic functions?**

Correctly Identified	Needs Revision	Inappropriate	Mean	Standard Deviation	Standard Error	95% Confidence Interval
94%	6%	0%	2.944	.2357	.0556	2.827 – 3.062

**13. How often do you employ principles of common computer and network organizations, principles of common security models, and evaluation techniques?**

Correctly Identified	Needs Revision	Inappropriate	Mean	Standard Deviation	Standard Error	95% Confidence Interval
88%	12%	0%	2.889	.3234	.0762	2.728 – 3.050

**14. How often are you confronted with common flaws and security issues associated with systems architecture and design?**

Correctly Identified	Needs Revision	Inappropriate	Mean	Standard Deviation	Standard Error	95% Confidence Interval
55%	39%	6%	2.500	.6183	.1457	2.193 – 2.807

This question was revised and submitted in round 2

**15. How often do you employ systems architecture evaluation techniques?**

Correctly Identified	Needs Revision	Inappropriate	Mean	Standard Deviation	Standard Error	95% Confidence Interval
83%	17%	0%	2.833	.3835	.0904	2.643 – 3.000

**16. How often do you employ administrative management concepts, resource protection, audit trails, inappropriate activities, violations, breaches, and reporting?**

Correctly Identified	Needs Revision	Inappropriate	Mean	Standard Deviation	Standard Error	95% Confidence Interval
83%	17%	0%	2.833	.3835	.0904	2.643 – 3.000

**17. How often do you employ monitoring tools and techniques, intrusion detection and penetration detection techniques, threats and counter measures?**

Correctly Identified	Needs Revision	Inappropriate	Mean	Standard Deviation	Standard Error	95% Confidence Interval
100%	0%	0%	N/A	N/A	N/A	N/A

**18. How often do you employ protection of critical business processes?**

Correctly Identified	Needs Revision	Inappropriate	Mean	Standard Deviation	Standard Error	95% Confidence Interval
94%	6%	0%	2.944	.2291	.0526	2.834 – 3.055

**19. How often do you employ procedures for emergency response, extended back-up and post-disaster recovery?**

Correctly Identified	Needs Revision	Inappropriate	Mean	Standard Deviation	Standard Error	95% Confidence Interval
100%	0%	0%	N/A	N/A	N/A	N/A

**20. How often do you address the issue of computer crime?**

Correctly Identified	Needs Revision	Inappropriate	Mean	Standard Deviation	Standard Error	95% Confidence Interval
55%	39%	11%	2.500	.6183	.1457	2.193 – 2.807

This question was revised and submitted in round 2

**21. How often do you employ information security incident handling and investigations?**

Correctly Identified	Needs Revision	Inappropriate	Mean	Standard Deviation	Standard Error	95% Confidence Interval
94%	6%	0%	2.944	.2357	.0556	2.827 – 3.005

**22. How often do you employ the concepts of computer ethics?**

Correctly Identified	Needs Revision	Inappropriate	Mean	Standard Deviation	Standard Error	95% Confidence Interval
94%	6%	0%	2.947	.2233	.0499	2.834 – 3.052

**23. How often do you employ facility requirements, environment and life safety?**

Correctly Identified	Needs Revision	Inappropriate	Mean	Standard Deviation	Standard Error	95% Confidence Interval
0%	0%	100%	N/A	N/A	N/A	N/A

This item was removed from the survey.

**24. How often do you employ the concepts of protection from physical security threats?**

Correctly Identified	Needs Revision	Inappropriate	Mean	Standard Deviation	Standard Error	95% Confidence Interval
100%	0%	0%	N/A	N/A	N/A	N/A



## Appendix J

### Validity E-mail Round Two

Subject: University Info Sec Research

Dear Colleague:

Thank you for submitting your initial response for the content validity survey. This response from you and the other content validity panel members identified three questions for revision. These questions and the revisions are included at the Web site identified below. Please review these revised questions using the following criteria:

- 1) Accept the revision, no comments
- 2) Accept the revision, with comments
- 3) Reject the revision, with comments

Please log on to <http://cob.bloomu.edu/afundaburk/content> to participate in this process. Your prompt action in responding by October 13, 2003 will be greatly appreciated

PIN: <PIN>

Again, I would like to thank you for taking the time to participate in this validation process. If you have any questions, please contact me.

Al Fundaburk  
Assistant Professor  
Business Education/Office Information Systems  
Bloomsburg University  
Bloomsburg, PA 17815  
(570) 389-4816  
[afundabr@bloomu.edu](mailto:afundabr@bloomu.edu)

## Appendix K

## Validity Survey Round Two

<b>Question 5 revision: How often have you employed security controls when addressing communications and network security, Internet/Intranet/Extranet, e-mail security, facsimile security, secure voice communications, and security boundaries?</b>		
Accept the revision, no comments	accept the revision, with comments	reject the revision, with comments
()	()	()
Comments:		

<b>Question 14 revision: How often are you confronted with common flaws and security issues associated with systems architecture and design?</b>		
Accept the revision, no comments	accept the revision, with comments	reject the revision, with comments
()	()	()
Comments:		

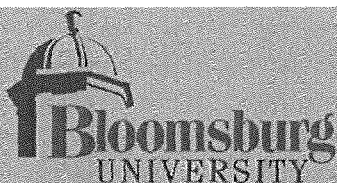
<b>Question 20 revision: How often do you address the issue of computer crime?</b>		
Accept the revision, no comments	accept the revision, with comments	reject the revision, with comments
()	()	()
Comments:		

## Appendix L

## Validity Results Round Two

<b>Question 5 revision: How often have you employed security controls when addressing communications and network security, Internet/Intranet/Extranet, e-mail security, facsimile security, secure voice communications, and security boundaries?</b>			
Accept the revision, no comments	accept the revision, with comments	reject the revision, with comments	Comments
93%	7%	0%	I believe that the question may be too generic. Most organizations employ some sort of malicious code identifier, but may not use more comprehensive security architecture. I believe that responses could be misleading.
<b>Question 14 revision: How often are you confronted with common flaws and security issues associated with systems architecture and design?</b>			
Accept the revision, no comments	accept the revision, with comments	reject the revision, with comments	Comments
100%	0%	0%	N/A
<b>Question 20 revision: How often do you address the issue of computer crime?</b>			
Accept the revision, no comments	accept the revision, with comments	reject the revision, with comments	Comments
93%	7%	0%	Suggest you add a generic definition of computer crime

Appendix M  
IRB Approvals



School of Graduate Studies

November 17, 2003

TO: Albert Fundaburk  
Business Education/Office Information Systems

FROM: Jerrold R. Harris *J. Harris (R)*  
IRB Administrator and  
Director of Research and Sponsored Programs

Serial Number: 725

SUBJECT: Request for Exemption from Human Subjects Research Review

TITLE: *The Education of Information Security Professionals: An Analysis of Industry Needs vs. Academic Curriculum in the 21<sup>st</sup> Century*

I have reviewed your proposal and find that it meets the following exemption criteria:  
45CRF46.101(b)2.

Research involving the use of educational tests (cognitive, diagnostic, aptitude, achievement), survey procedures, interview procedures or observation of public behavior, unless: (i) Information obtained is recorded in such a manner that human subjects can be identified, directory or through identifiers linked to the subjects; and (ii) any disclosure of the human subjects' responses outside the research could reasonably place the subjects at risk of criminal or civil liability or be damaging to the subjects' financial standing, employability, or reputation.

cc: IRB chair

**AI Fundaburk**

**From:** James Cannady [j.cannady@computer.org]  
**Sent:** Saturday, November 15, 2003 1:08 PM  
**To:** fundabur@nova.edu  
**Subject:** IRB Approval  
**Importance:** High

AI,

After reviewing your IRB Submission Form and Research Protocol I have approved your proposed research for IRB purposes. Your research has been determined to be exempt from further IRB review based on the following conclusion:

Research using survey procedures or interview procedures where subjects' identities are thoroughly protected and their answers do not subject them to criminal and civil liability.

Please note that while your research has been approved, additional IRB reviews of your research will be required if any of the following circumstances occur:

1. If you, during the course of conducting your research, revise the research protocol (e.g., making changes to the informed consent form, survey instruments used, or number and nature of subjects).
2. If the portion of your research involving human subjects exceeds 12 months in duration.

Please feel free to contact me in the future if you have any questions regarding my evaluation of your research or the IRB process.

Dr. Cannady

---

James Cannady, Ph.D.  
Assistant Professor

Graduate School of Computer  
and Information Sciences  
Nova Southeastern University

954.262.2085  
404.312.2374 (mobile phone)  
cannady@nova.edu

PGP public key fingerprint:  
8169 6D03 680E EF6C 899C  
8C42 B4A3 DC9F 9F6B 4075

---

Appendix N  
Survey E-Mails

Dear Colleague,

I am in the process of completing my dissertation for a Doctorate in Information Systems. I am asking for your assistance in completing a survey which will be used to compare the tasks performed by information security professionals in the field with the skills being taught in the information security curriculum in schools designated as National Security Agency (NSA) Centers of Excellence in Information Assurance.

You were chosen to participate because you teach in an NSA designated School of Excellence in Information Assurance. Participation is totally voluntary and should take no longer than 10 minutes of your time. Since the validity of the results depend on obtaining a high response rate, your participation is crucial to the success of this research. I, as the principal researcher, will be the only person viewing the collected data and to ensure anonymity all links to PINs will be deleted at the conclusion of data collection. If you know of other faculty, teaching this curriculum, who did not receive this e-mail, please forward and have them use the PIN "12345".

Colleges and universities will be able to use the results of this research to improve information security courses to address real world needs. In addition, the survey results will be made available to the International Information Systems Security Certification Consortium. If you wish to obtain the results of this survey so indicate on the on-line form available at the end of the survey.

Please log on to <http://cob.bloomu.edu/afundaburk/infosecsurvey> and use the Personal Identification Number <PIN> to participate. Your response by December 21, 2003 will be greatly appreciated.

Thank you for your help in this needed research. If you have any questions, please contact me.

Al Fundaburk  
Assistant Professor  
Business Education/Office Information Systems  
Bloomsburg University  
Bloomsburg, PA 17815  
(570) 389-4816  
afundabr@bloomu.edu



Dear Colleague,

I am in the process of completing my dissertation for a Doctorate in Information Systems. I am asking for your assistance in completing a survey which will be used to compare the tasks performed by information security professionals in the field with the skills being taught in the information security curriculum in schools designated as National Security Agency (NSA) Centers of Excellence in Information Assurance.

You were chosen to participate because of your expertise in the field of information security and your CISSP certification. Participation is totally voluntary and should take no longer than 10 minutes of your time. Since the validity of the results depend on obtaining a high response rate, your participation is crucial to the success of this research. I, as the principal researcher, will be the only person viewing the collected data and to ensure anonymity all links to PINs will be deleted at the conclusion of data collection.

Colleges and universities will be able to use the results of this research to improve information security courses to address real world needs. In addition, the survey results will be made available to the International Information Systems Security Certification Consortium. If you wish to obtain the results of this survey so indicate on the on-line form available at the end of the survey.

Please log on to <http://cob.bloomu.edu/afundaburk/infosecsurvey> and use the Personal Identification Number <PIN> to participate. Your response by December 21, 2003 will be greatly appreciated.

Thank you for your help in this needed research. If you have any questions, please contact me.

Al Fundaburk  
Assistant Professor  
Business Education/Office Information Systems  
Bloomsburg University  
Bloomsburg, PA 17815  
(570) 389-4816  
afundabr@bloomu.edu

Dear Colleague,

Ten days ago you should have received an online survey concerning tasks taught by information security faculty in NSA Schools of Excellence in Information Assurance. Your ideas and experience will make a valuable contribution to my dissertation research. Will you please take the time now to fill out this short survey?

Log on to <http://cob.bloomu.edu/afundaburk/infosecsurvey> and use the Personal Identification Number <PIN> to participate. Thank you for your help. If you have questions, please contact me.

Al Fundaburk  
Assistant Professor  
Business Education/Office Information Systems  
Bloomsburg University  
Bloomsburg, PA 17815  
(570) 389-4816  
[afundabr@bloomu.edu](mailto:afundabr@bloomu.edu)

Dear Colleague,

Ten days ago you should have received an online survey concerning tasks performed by information security professionals in the field. Your ideas and experience will make a valuable contribution to my dissertation research. Will you please take the time now to fill out this short survey?

Log on to <http://cob.bloomu.edu/afundaburk/infosecsurvey> and use the Personal Identification Number <PIN> to participate. Thank you for your help. If you have questions, please contact me.

Al Fundaburk  
Assistant Professor  
Business Education/Office Information Systems  
Bloomsburg University  
Bloomsburg, PA 17815  
(570) 389-4816  
[afundabr@bloomu.edu](mailto:afundabr@bloomu.edu)

Dear Colleague,

Ten days ago you should have received my second request to complete an online survey concerning tasks taught by information security faculty in NSA Schools of Excellence in Information Assurance. I truly value your ideas and experience. Your taking the time to complete this survey will make a valuable contribution to information security research. Will you please take the time now to fill out this short survey?

Log on to <http://cob.bloomu.edu/afundaburk/infosecsurvey> and use the Personal Identification Number <PIN> to participate. Thank you for your help. If you have questions, please contact me.

Al Fundaburk  
Assistant Professor  
Business Education/Office Information Systems  
Bloomsburg University  
Bloomsburg, PA 17815  
(570) 389-4816  
afundabr@bloomu.edu

Dear Colleague,

Ten days ago you should have received my second request to complete an online survey concerning tasks performed by information security professionals in the field. I truly value your ideas and experience. Your taking the time to complete this survey will make a valuable contribution to information security research. Will you please take the time now to fill out this short survey?

Log on to <http://cob.bloomu.edu/afundaburk/infosecsurvey> and use the Personal Identification Number <PIN> to participate. Thank you for your help. If you have questions, please contact me.

Al Fundaburk  
Assistant Professor  
Business Education/Office Information Systems  
Bloomsburg University  
Bloomsburg, PA 17815  
(570) 389-4816  
afundabr@bloomu.edu

## Appendix O

### Information Systems Security Faculty Survey

The following questions will provide background information of respondents. The assignment of the PIN allows for individual and institutional anonymity. The participant database and survey responses will be kept confidential by the principal researcher. After survey completion, the database linking PINs to participants will be deleted assuring participant anonymity.

Please select all that apply:

- I have published textbook(s) or article(s) in the area of information security.
- I have participated in at least one national or state convention as a speaker or panel member discussing the topic of information security.
- I am a member of the faculty of an accredited university with a viable information security curriculum.
- I hold a CISSP certification.

Click here if none of the above applies to you,

Otherwise, please input PIN here:                      and click on submit.

Submit

The purpose of this survey is to compare the skills and attributes identified in the ten domains of the CISSP being taught in a designated NSA “Centers of Excellence” security curriculum to the skills and attributes employed by professionals working in an information security environment. As a participant you will be asked to fill out a survey about your teaching of specific information security skills. This survey is being conducted as part of a dissertation titled: *The Education of Information Security Professionals: An Analysis of Industry Needs vs. Academic Curriculum in the 21<sup>st</sup> Century*. The principal researcher is the only person viewing the collected data and all links to PINs will be deleted at the conclusion of data collection. Participation in this survey is totally voluntary and should take no longer than 10 minutes.

The following questions are about information security skills. How often do you teach the following skills in your information security curriculum? Please click on the corresponding radio button that identifies the frequency. At the completion of each question, click on the submit button to record your answer.

1. How often do you teach access control techniques, access control administration, and access control models?

Always       Often       Sometimes       Rarely       Never

2. How often do you teach identification and authentication techniques?

Always       Often       Sometimes       Rarely       Never

3. How often do you teach intrusion detection monitoring, and penetration testing?

Always       Often       Sometimes       Rarely       Never

4. How often do you teach International Standards Organization/Open Systems Interconnection, Layers and characteristics?

Always       Often       Sometimes       Rarely       Never

5. How often do you teach communications and network security, Internet/Intranet/Extranet, e-mail security, facsimile security, secure voice communications, and security boundaries?

Always       Often       Sometimes       Rarely       Never

6. How often do you teach implementation and management of change control?

Always       Often       Sometimes       Rarely       Never

7. How often do you teach the development or implementation of information security employment policies, practices, standards, guidelines, and procedures?

Always       Often       Sometimes       Rarely       Never

8. How often do you teach security awareness training and management?

Always       Often       Sometimes       Rarely       Never

9. How often do you teach information security involving database and data warehousing, and information storage?

Always  Often  Sometimes  Rarely  Never

10. How often do you teach information security regarding knowledge based systems and development controls?

Always  Often  Sometimes  Rarely  Never

11. How often do you teach cryptographic concepts, methodologies and practices, private and public key algorithms, and public key infrastructure?

Always  Often  Sometimes  Rarely  Never

12. How often do you teach system architecture for implementing cryptographic functions?

Always  Often  Sometimes  Rarely  Never

13. How often do you teach principles of common computer and network organizations, principles of common security models, and evaluation techniques?

Always  Often  Sometimes  Rarely  Never

14. How often do you teach common flaws and security issues associated with systems architecture and design?

Always  Often  Sometimes  Rarely  Never

15. How often do you teach systems architecture evaluation techniques?

Always  Often  Sometimes  Rarely  Never

16. How often do you teach administrative management concepts, resource protection, audit trails, inappropriate activities, violations, breaches, and reporting?

Always  Often  Sometimes  Rarely  Never

17. How often do you teach monitoring tools and techniques, intrusion detection and penetration detection techniques, threats and counter measures?

Always  Often  Sometimes  Rarely  Never

18. How often do you teach protection of critical business processes?

Always  Often  Sometimes  Rarely  Never

19. How often do you teach procedures for emergency response, extended back-up and post-disaster recovery?

Always  Often  Sometimes  Rarely  Never

20. How often do you teach the aspects of computer crime?

Always  Often  Sometimes  Rarely  Never



21. How often do you teach information security incident handling and investigations?

Always       Often       Sometimes       Rarely       Never

22. How often do you teach the concepts of computer ethics?

Always       Often       Sometimes       Rarely       Never

23. How often do you teach the concepts of protection from physical security threats?

Always       Often       Sometimes       Rarely       Never

## Appendix P

### Information Systems Security Professional Survey

The following questions will provide background information of respondents. The assignment of the PIN allows for individual and institutional anonymity. The participant database and survey responses will be kept confidential by the principal researcher. After survey completion, the database linking PINs to participants will be deleted assuring participant anonymity.

To participate in this survey you must be a member of the faculty of an accredited university with a viable information security program. If not please [click here](#) to exit the survey.

Please click on the radio buttons below if applicable:

- I have published textbook(s) or article(s) in the area of information security
  
- I have participated in national or state convention as a speaker or panel member discussing the topic of information security
  
- I hold a CISSP certification

To participate please input PIN here: \_\_\_\_\_ and click on submit.

Submit

The purpose of this survey is to compare the skills and attributes identified in the ten domains of the CISSP to the skills and attributes employed by professionals working in an information security environment. As a participant you will be asked to fill out a survey about your use of specific information security skills. This survey is being conducted as part of a dissertation titled: *The Education of Information Security Professionals: An Analysis of Industry Needs vs. Academic Curriculum in the 21<sup>st</sup> Century*. The principal researcher is the only person viewing the collected data and all links to PINs will be deleted at the conclusion of data collection. Participation in this survey is totally voluntary and should take no longer than 10 minutes.

The following questions are about information security skills. How often do you employ the following skills while working in an information security environment? Please click on the corresponding radio button that identifies the frequency. At the completion of each question, click on the submit button to record your answer.

1. How often do you employ access control techniques, access control administration, and access control models?

Always       Often       Sometimes       Rarely       Never

2. How often do you employ identification and authentication techniques?

Always       Often       Sometimes       Rarely       Never

3. How often do you employ intrusion detection monitoring and penetration testing?

Always       Often       Sometimes       Rarely       Never

4. How often do you employ International Standards Organization/Open Systems Interconnection, Layers and characteristics?

Always       Often       Sometimes       Rarely       Never

5. How often have you employed security controls when addressing communications and network security, Internet/Intranet/Extranet, e-mail security, facsimile security, secure voice communications, and security boundaries?

Always       Often       Sometimes       Rarely       Never

6. How often do you employ implementation and management of change control?

Always       Often       Sometimes       Rarely       Never

7. How often do you employ the development or implementation of information security employment policies, practices, standards, guidelines, and procedures?

Always       Often       Sometimes       Rarely       Never

8. How often do you employ security awareness training and management?

Always       Often       Sometimes       Rarely       Never

9. How often do you employ information security involving database and data warehousing, and information storage?

Always  Often  Sometimes  Rarely  Never

10. How often do you employ information security regarding knowledge based systems and development controls?

Always  Often  Sometimes  Rarely  Never

11. How often do you employ cryptographic concepts, methodologies and practices, private and public key algorithms, and public key infrastructure?

Always  Often  Sometimes  Rarely  Never

12. How often do you employ system architecture for implementing cryptographic functions?

Always  Often  Sometimes  Rarely  Never

13. How often do you employ principles of common computer and network organizations, principles of common security models, and evaluation techniques?

Always  Often  Sometimes  Rarely  Never

14. How often are you confronted with common flaws and security issues associated with systems architecture and design?

Always  Often  Sometimes  Rarely  Never

15. How often do you employ systems architecture evaluation techniques?

Always  Often  Sometimes  Rarely  Never

16. How often do you employ administrative management concepts, resource protection, audit trails, inappropriate activities, violations, breaches, and reporting?

Always  Often  Sometimes  Rarely  Never

17. How often do you employ monitoring tools and techniques, intrusion detection and penetration detection techniques, threats and counter measures?

Always  Often  Sometimes  Rarely  Never

18. How often do you employ protection of critical business processes?

Always  Often  Sometimes  Rarely  Never

19. How often do you employ procedures for emergency response, extended back-up and post-disaster recovery?

Always  Often  Sometimes  Rarely  Never

20. How often do you address the issue of computer crime?

Always  Often  Sometimes  Rarely  Never

21. How often do you employ information security incident handling and investigations?

Always       Often       Sometimes       Rarely       Never

22. How often do you employ the concepts of computer ethics?

Always       Often       Sometimes       Rarely       Never

23. How often do you employ the concepts of protection from physical security threats?

Always       Often       Sometimes       Rarely       Never

Appendix Q  
SPSS Statistical Results

## Questions pro1 and edu1

### Statistics

		PRO1	EDU1
N	Valid	125	99
	Missing	0	26
Mean		4.6080	3.7172
Std. Error of Mean		.05553	.13005
Median		5.0000	4.0000
Skewness		-1.550	-.839
Std. Error of Skewness		.217	.243

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	2.843 <sup>a</sup>	9	.970
Likelihood Ratio	3.470	9	.943
Linear-by-Linear Association	.173	1	.677
N of Valid Cases	99		

a 9 cells (56.3%) have expected count less than 5. The minimum expected count is .12.

### Symmetric Measures

		Value	Asymp. Std. Error <sup>a</sup>	Approx. T <sup>b</sup>	Approx. Sig.
Ordinal by Ordinal	Kendall's tau-b	-.013	.091	-.141	.888
N of Valid Cases		99			

a Not assuming the null hypothesis.

b Using the asymptotic standard error assuming the null hypothesis.

### Test Statistics<sup>b</sup>

Z	EDU1 - PRO1 -5.486 <sup>a</sup>
---	------------------------------------

Asymp. .000  
Sig. (2-  
tailed)

a Based on positive ranks.

b Wilcoxon Signed Ranks Test

### Questions pro2 and edu2

#### Statistics

		PRO2	EDU2
N	Valid	125	99
	Missing	0	26
Mean		4.6480	3.8990
Std. Error of Mean		.04580	.12639
Skewness		-.990	-1.220
Std. Error of Skewness		.217	.243
Minimum		3.00	1.00
Maximum		5.00	5.00

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2- sided)
Pearson Chi-Square	4.198 <sup>a</sup>	8	.839
Likelihood Ratio	4.681	8	.791
Linear-by-Linear Association	1.073	1	.300
N of Valid Cases	99		

a 9 cells (60.0%) have expected count less than 5. The minimum expected count is .01.

#### Symmetric Measures

		Value	Asymp. Std. Error <sup>a</sup>	Approx. T <sup>b</sup>	Approx. Sig.
Ordinal by Ordinal	Kendall's tau-b	.109	.091	1.203	.229
N of Valid		99			



---

Cases

---

- a Not assuming the null hypothesis.  
b Using the asymptotic standard error assuming the null hypothesis.

---

Test Statistics

---

	EDU2 - PRO2
Z	-5.116
Asymp. Sig. (2- tailed)	.000

---

- a Based on positive ranks.  
b Wilcoxon Signed Ranks Test

**Question pro3 and edu3**


---

Statistics

---

		PRO3	EDU3
N	Valid	125	99
	Missing	0	26
Mean		4.0080	3.7576
Std. Error of Mean		.08762	.12275
Skewness		-1.115	-.653
Std. Error of Skewness		.217	.243
Minimum		1.00	1.00
Maximum		5.00	5.00

---



---

Chi-Square Tests

---

	Value	df	Asymp. Sig. (2- sided)
Pearson Chi- Square	17.762 <sup>a</sup>	16	.338
Likelihood Ratio	12.850	16	.684
Linear-by- Linear Associatio n	1.052	1	.305
N of Valid Cases	99		

---

- a 18 cells (72.0%) have expected count less than 5. The minimum expected count is .08.

## Symmetric Measures

		Value	Asymp. Std. Error <sup>a</sup>	Approx. T <sup>b</sup>	Approx. Sig.
Ordinal by Ordinal	Kendall's tau-b	.052	.091	.575	.566
Ordinal N of Valid Cases		99			

a Not assuming the null hypothesis.

b Using the asymptotic standard error assuming the null hypothesis.

Test Statistics<sup>b</sup>

		EDU3 - PRO3
Z		-2.096 <sup>a</sup>
Asymp. Sig. (2- tailed)		.036

a Based on positive ranks.

b Wilcoxon Signed Ranks Test

## Questions pro4 and edu4

## Statistics

		PRO4	EDU4
N	Valid	125	99
	Missing	0	26
Mean		4.1840	3.6768
Std. Error of Mean		.04455	.10336
Skewness		.347	-.691
Std. Error of Skewness		.217	.243
Minimum		3.00	1.00
Maximum		5.00	5.00

## Chi-Square Tests

		Value	df	Asymp. Sig. (2- sided)
Pearson Chi-		4.410 <sup>a</sup>	8	.818

Square Likelihood Ratio	5.915	8	.657
Linear-by-Linear Association	1.290	1	.256
N of Valid Cases	99		

a 8 cells (53.3%) have expected count less than 5. The minimum expected count is .16.

#### Symmetric Measures

	Value	Asymp. Std. Error <sup>a</sup>	Approx. T <sup>b</sup>	Approx. Sig.
Ordinal by Ordinal Kendall's tau-b	.104	.082	1.266	.206
N of Valid Cases	99			

a Not assuming the null hypothesis.

b Using the asymptotic standard error assuming the null hypothesis.

#### Test Statistics<sup>b</sup>

	EDU4 - PRO4
Z	-4.424 <sup>a</sup>
Asymp. Sig. (2-tailed)	.000

a Based on positive ranks.

b Wilcoxon Signed Ranks Test

#### Question pro5 and edu5

##### Statistics

	PRO5	EDU5
N	125	99
Valid	125	99
Missing	0	26
Mean	4.3920	3.9596
Std. Error of Mean	.06415	.10543
Median	5.0000	4.0000
Skewness	-.745	-.676

Std. Error of Skewness	.217	.243
Minimum	3.00	2.00
Maximum	5.00	5.00

## Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	6.213 <sup>a</sup>	6	.400
Likelihood Ratio	6.474	6	.372
Linear-by-Linear Association	.550	1	.458
N of Valid Cases	99		

a 4 cells (33.3%) have expected count less than 5. The minimum expected count is 2.12.

## Symmetric Measures

	Value	Asymp. Std. Error <sup>a</sup>	Approx. T <sup>b</sup>	Approx. Sig.
Ordinal by Ordinal Kendall's tau-b	-.072	.089	-.801	.423
N of Valid Cases	99			

a Not assuming the null hypothesis.

b Using the asymptotic standard error assuming the null hypothesis.

Test Statistics<sup>b</sup>

EDU5 - PRO5	
Z	-2.840 <sup>a</sup>
Asymp. Sig. (2-tailed)	.005

a Based on positive ranks.

b Wilcoxon Signed Ranks Test

## Questions pro6 and edu6

### Statistics

		PRO6	EDU6
N	Valid	125	99
	Missing	0	26
Mean		4.0000	2.7778
Std. Error of Mean		.07449	.14398
Skewness		-.426	.401
Std. Error of Skewness		.217	.243
Minimum		2.00	1.00
Maximum		5.00	5.00

### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	9.433 <sup>a</sup>	9	.398
Likelihood Ratio	11.148	9	.266
Linear-by-Linear Association	.332	1	.565
N of Valid Cases	99		

a 7 cells (43.8%) have expected count less than 5. The minimum expected count is 1.11.

### Symmetric Measures

		Value	Asymp. Std. Error <sup>a</sup>	Approx. T <sup>b</sup>	Approx. Sig.
Ordinal by Ordinal	Kendall's tau-b	-.035	.089	-.389	.697
N of Valid Cases		99			

a Not assuming the null hypothesis.

b Using the asymptotic standard error assuming the null hypothesis.

### Test Statistics<sup>b</sup>

EDU6 -

---

	PRO6
Z	-5.800 <sup>a</sup>
Asymp. Sig. (2- tailed)	.000

---

a Based on positive ranks.

b Wilcoxon Signed Ranks Test

### Question pro7 and edu7

#### Statistics

---

		PRO7	EDU7
N	Valid	125	99
	Missing	0	26
Mean		4.1760	4.0303
Std. Error of Mean		.06331	.12878
Skewness		-.265	-1.067
Std. Error of Skewness		.217	.243
Minimum		3.00	1.00
Maximum		5.00	5.00

---

#### Chi-Square Tests

---

	Value	df	Asymp. Sig. (2- sided)
Pearson Chi-Square	8.735 <sup>a</sup>	8	.365
Likelihood Ratio	10.525	8	.230
Linear-by-Linear Association	.002	1	.968
N of Valid Cases	99		

---

a 9 cells (60.0%) have expected count less than 5. The minimum expected count is 1.21.

#### Symmetric Measures

---

		Value	Asymp. Std. Error <sup>a</sup>	Approx. T <sup>b</sup>	Approx. Sig.
Ordinal by Ordinal	Kendall's tau-b	.003	.083	.031	.975
N of		99			

---

Valid  
Cases

a Not assuming the null hypothesis.

b Using the asymptotic standard error assuming the null hypothesis.

Test Statistics<sup>b</sup>

	EDU7 - PRO7
Z	-.628 <sup>a</sup>
Asymp. Sig. (2- tailed)	.530

a Based on positive ranks.

b Wilcoxon Signed Ranks Test

### Questions pro8 and edu8

Descriptive Statistics

		PRO8	EDU8
N	Valid	125	99
	Missing	0	26
Mean		3.8240	3.8889
Std. Error of Mean		.07625	.11566
Std. Deviation		.85255	1.15077
Skewness		-.129	-1.009
Std. Error of Skewness		.217	.243
Minimum		2.00	1.00
Maximum		5.00	5.00

Chi-Square Tests

	Value	df	Asymp. Sig. (2- sided)
Pearson Chi-Square	6.152 <sup>a</sup>	12	.908
Likelihood Ratio	7.382	12	.831
Linear-by- Linear Association	.584	1	.445
N of Valid Cases	99		

a 11 cells (55.0%) have expected count less than 5. The minimum expected count is .10.

#### Symmetric Measures

		Value	Asymp. Std. Error <sup>a</sup>	Approx. T <sup>b</sup>	Approx. Sig.
Ordinal	Kendall's	.089	.087	1.019	.308
by	tau-b				
Ordinal					
N of		99			
Valid					
Cases					

a Not assuming the null hypothesis.

b Using the asymptotic standard error assuming the null hypothesis.

#### Test Statistics<sup>b</sup>

	EDU8 - PRO8
Z	-1.165 <sup>a</sup>
Asymp. Sig. (2- tailed)	.244

a Based on negative ranks.

b Wilcoxon Signed Ranks Test

#### Questions pro9 and edu9

#### Statistics

		PRO9	EDU9
N	Valid	125	99
	Missing	0	26
Mean		4.0080	3.6768
Std. Error of Mean		.08230	.11998
Std. Deviation		.92017	1.19376
Skewness		-.963	-.448
Std. Error of Skewness		.217	.243
Minimum		1.00	1.00
Maximum		5.00	5.00

#### Chi-Square Tests

Value	df	Asymp. Sig. (2-
-------	----	--------------------



Pearson Chi-Square	37.058 <sup>a</sup>	16	.002	sided)
Likelihood Ratio	29.130	16	.023	
Linear-by-Linear Association	4.245	1	.039	
N of Valid Cases	99			

a 16 cells (64.0%) have expected count less than 5. The minimum expected count is .06.

#### Symmetric Measures

		Value	Asymp. Std. Error <sup>a</sup>	Approx. T <sup>b</sup>	Approx. Sig.
Ordinal by Ordinal	Kendall's tau-b	.127	.084	1.503	.133
N of Valid Cases		99			

a Not assuming the null hypothesis.

b Using the asymptotic standard error assuming the null hypothesis.

#### Test Statistics<sup>b</sup>

	EDU9 - PRO9
Z	-2.463 <sup>a</sup>
Asymp. Sig. (2-tailed)	.014

a Based on positive ranks.

b Wilcoxon Signed Ranks Test

#### Questions pro10 and edu10

##### Statistics

		PRO10	EDU10
N	Valid	125	99
	Missing	0	26
Mean		3.4560	3.2222
Std. Error of Mean		.09538	.10507
Std. Deviation		1.06638	1.04545

Skewness	-.147	.251
Std. Error of Skewness	.217	.243
Minimum	1.00	1.00
Maximum	5.00	5.00

## Chi-Square Tests

	Value	Asymp. Sig. (2- sided)	df
Pearson Chi- Square	22.802 <sup>a</sup>	.029	12
Likelihood Ratio	20.462	.059	12
Linear- by-Linear Association	2.659	.103	1
N of Valid Cases	99		

a 14 cells (70.0%) have expected count less than 5. The minimum expected count is .08.

## Symmetric Measures

	Value	Asymp. Std. Error <sup>a</sup>	Approx. T <sup>b</sup>	Approx. Sig.
Ordinal by Ordinal Kendall's tau-b	.121	.092	1.304	.192
N of Valid Cases	99			

a Not assuming the null hypothesis.

b Using the asymptotic standard error assuming the null hypothesis.

Test Statistics<sup>b</sup>

	EDU10 - PRO10
Z	-2.146 <sup>a</sup>
Asymp. Sig. (2- tailed)	.032

a Based on positive ranks.

## b Wilcoxon Signed Ranks Test

**Questions pro11 and edu11**

## Statistics

		PRO11	EDU11
N	Valid	125	99
	Missing	0	26
Mean		3.6960	4.0808
Std. Error of Mean		.07023	.13055
Std. Deviation		.78519	1.29895
Skewness		-.419	-1.350
Std. Error of Skewness		.217	.243
Minimum		1.00	1.00
Maximum		5.00	5.00

## Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	16.371 <sup>a</sup>	16	.427
Likelihood Ratio	19.909	16	.224
Linear-by-Linear Association	.187	1	.665
N of Valid Cases	99		

a 19 cells (76.0%) have expected count less than 5. The minimum expected count is .02.

## Symmetric Measures

		Value	Asymp. Std. Error <sup>a</sup>	Approx. T <sup>b</sup>	Approx. Sig.
Ordinal by Ordinal	Kendall's tau-b	-.057	.087	-.655	.512
N of Valid Cases		99			

a Not assuming the null hypothesis.

b Using the asymptotic standard error assuming the null hypothesis.

Test Statistics <sup>b</sup>	
	EDU11 - PRO11
Z	-2.538 <sup>a</sup>
Asymp. Sig. (2- tailed)	.011

a Based on negative ranks.

b Wilcoxon Signed Ranks Test

### Questions pro12 and edu12

Statistics			
		PRO12	EDU12
N	Valid	125	99
	Missing	0	26
Mean		3.3200	3.0505
Std. Error of Mean		.08843	.13031
Std. Deviation		.98865	1.29657
Skewness		-.377	-.038
Std. Error of Skewness		.217	.243
Minimum		1.00	1.00
Maximum		5.00	5.00

Chi-Square Tests			
	Value	df	Asymp. Sig. (2- sided)
Pearson Chi- Square	13.451 <sup>a</sup>	16	.640
Likelihood Ratio	15.109	16	.517
Linear- by-Linear Association	.120	1	.729
N of Valid Cases	99		

a 16 cells (64.0%) have expected count less than 5. The minimum expected count is .57.

#### Symmetric Measures

	Value	Asymp. Std. Error <sup>a</sup>	Approx. T <sup>b</sup>	Approx. Sig.
Ordinal by Ordinal Kendall's tau-b	.039	.079	.500	.617
Ordinal N of Valid Cases	99			

a Not assuming the null hypothesis.

b Using the asymptotic standard error assuming the null hypothesis.

#### Test Statistics<sup>b</sup>

	EDU12 - PRO12
Z	-1.953 <sup>a</sup>
Asymp. Sig. (2- tailed)	.051

a Based on positive ranks.

b Wilcoxon Signed Ranks Test

#### Questions pro13 and edu13

##### Statistics

		PRO13	EDU13
N	Valid	125	99
	Missing	0	26
Mean		3.9440	3.9798
Std. Error of Mean		.07388	.13993
Std. Deviation		.82603	1.39225
Skewness		-.418	-1.190
Std. Error of Skewness		.217	.243
Minimum		2.00	1.00
Maximum		5.00	5.00

##### Chi-Square Tests

	Value	df	Asymp. Sig. (2-

			sided)
Pearson Chi-Square	17.137	12	.145
Likelihood Ratio	21.288	12	.046
Linear-by-Linear Association	1.012	1	.315
N of Valid Cases	99		

a 14 cells (70.0%) have expected count less than 5. The minimum expected count is .06.

#### Symmetric Measures

	Value	Asymp. Std. Error <sup>a</sup>	Approx. T <sup>b</sup>	Approx. Sig.
Ordinal by Ordinal Kendall's tau-b	.095	.080	1.175	.240
Ordinal N of Valid Cases	99			

a Not assuming the null hypothesis.

b Using the asymptotic standard error assuming the null hypothesis.

#### Test Statistics<sup>b</sup>

	EDU13 - PRO13
Z	-.576 <sup>a</sup>
Asymp. Sig. (2-tailed)	.564

a Based on negative ranks.

b Wilcoxon Signed Ranks Test

#### Questions pro14 and edu14

##### Statistics

	PRO14	EDU14
N	125	99
Valid		
Missing	0	26
Mean	4.1520	3.9091
Std. Error of Mean	.05909	.14001
Std. Deviation	.66060	1.39307

Skewness	-.344	-1.106
Std. Error of Skewness	.217	.243
Minimum	2.00	1.00
Maximum	5.00	5.00

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	13.126 <sup>a</sup>	12	.360
Likelihood Ratio	13.846	12	.311
Linear-by-Linear Association	.317	1	.573
N of Valid Cases	99		

a 13 cells (65.0%) have expected count less than 5. The minimum expected count is .03.

#### Symmetric Measures

	Value	Asymp. Std. Error <sup>a</sup>	Approx. T <sup>b</sup>	Approx. Sig.
Ordinal by Ordinal Kendall's tau-b	.063	.077	.829	.407
N of Valid Cases	99			

a Not assuming the null hypothesis.

b Using the asymptotic standard error assuming the null hypothesis.

#### Test Statistics<sup>b</sup>

	EDU14 - PRO14
Z	-1.371 <sup>a</sup>
Asymp. Sig. (2-tailed)	.170

a Based on positive ranks.

b Wilcoxon Signed Ranks Test

#### Questions pro15 and edu15

Statistics		PRO15	EDU15
N	Valid	125	99
	Missing	0	26
Mean		3.5680	3.1313
Std. Error of Mean		.07815	.11633
Std. Deviation		.87378	1.15746
Skewness		-.064	-.060
Std. Error of Skewness		.217	.243
Minimum		1.00	1.00
Maximum		5.00	5.00

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	9.281 <sup>a</sup>	16	.901
Likelihood Ratio	10.609	16	.833
Linear-by-Linear Association	2.224	1	.136
N of Valid Cases	99		

a. 19 cells (76.0%) have expected count less than 5. The minimum expected count is .06.

Symmetric Measures					
		Value	Asymp. Std. Error <sup>a</sup>	Approx. T <sup>b</sup>	Approx. Sig.
Ordinal by Ordinal	Kendall's tau-b	.132	.085	1.532	.126
N of Valid Cases		99			

a. Not assuming the null hypothesis.



b Using the asymptotic standard error assuming the null hypothesis.

Test Statistics <sup>b</sup>	
	EDU15 - PRO15
Z	-3.176 <sup>a</sup>
Asymp. Sig. (2-tailed)	.001

a Based on positive ranks.

b Wilcoxon Signed Ranks Test

### Questions pro16 and edu16

Statistics			
		PRO16	EDU16
N	Valid	125	99
	Missing	0	26
Mean		4.1200	3.4343
Std. Error of Mean		.04899	.13932
Std. Deviation		.54772	1.38624
Skewness		.069	-.283
Std. Error of Skewness		.217	.243
Minimum		3.00	1.00
Maximum		5.00	5.00

Chi-Square Tests			
	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	5.867 <sup>a</sup>	6	.438
Likelihood Ratio	5.790	6	.447
Linear-by-Linear Association	3.239	1	.072
N of Valid Cases	99		

a 7 cells (58.3%) have expected count less than 5. The minimum expected count is .30.

### Symmetric Measures

	Value	Asymp. Std. Error <sup>a</sup>	Approx. T <sup>b</sup>	Approx. Sig.
Ordinal by Ordinal Kendall's tau-b	.177	.092	1.886	.059
N of Valid Cases	99			

a Not assuming the null hypothesis.

b Using the asymptotic standard error assuming the null hypothesis.

### Test Statistics<sup>b</sup>

	EDU16 - PRO16
Z	-4.367 <sup>a</sup>
Asymp. Sig. (2- tailed)	.000

a Based on positive ranks.

b Wilcoxon Signed Ranks Test

### Questions pro17 and edu17

#### Statistics

	PRO17	EDU17
N	125	99
Valid		
Missing	0	26
Mean	4.0480	3.9495
Std. Error of Mean	.07776	.13266
Std. Deviation	.86933	1.31997
Skewness	-1.142	-.802
Std. Error of Skewness	.217	.243
Minimum	1.00	1.00
Maximum	5.00	5.00

#### Chi-Square Tests

Value	df	Asymp. Sig. (2-
-------	----	--------------------

Pearson Chi-Square	22.077 <sup>a</sup>	12	.037
Likelihood Ratio	18.036	12	.115
Linear-by-Linear Association	3.232	1	.072
N of Valid Cases	99		

a 13 cells (65.0%) have expected count less than 5. The minimum expected count is .08.

Symmetric Measures

		Value	Asymp. Std. Error <sup>a</sup>	Approx. T <sup>b</sup>	Approx. Sig.
Ordinal by Ordinal	Kendall's tau-b	.109	.086	1.261	.207
N of Valid Cases		99			

a Not assuming the null hypothesis.

b Using the asymptotic standard error assuming the null hypothesis.

Test Statistics<sup>b</sup>

	EDU17 - PRO17
Z	-1.071 <sup>a</sup>
Asymp. Sig. (2-tailed)	.284

a Based on positive ranks.

b Wilcoxon Signed Ranks Test

Questions pro18 and edu18

Statistics

		PRO18	EDU18
N	Valid	125	99
	Missing	0	26
Mean		4.1680	3.3838
Std. Error		.06695	.13824

of Mean Std. Deviation	.74850	1.37549
Skewness Std. Error of Skewness	-.520 .217	-.221 .243
Minimum	2.00	1.00
Maximum	5.00	5.00

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2- sided)
Pearson Chi- Square	10.944 <sup>a</sup>	9	.280
Likelihood Ratio	9.075	9	.430
Linear- by-Linear Association	.741	1	.389
N of Valid Cases	99		

a 9 cells (56.3%) have expected count less than 5. The minimum expected count is .04.

#### Symmetric Measures

	Value	Asymp. Std. Error <sup>a</sup>	Approx. T <sup>b</sup>	Approx. Sig.
Ordinal by Ordinal Kendall's tau-b	-.109	.093	-1.174	.240
N of Valid Cases	99			

a Not assuming the null hypothesis.

b Using the asymptotic standard error assuming the null hypothesis.

#### Test Statistics<sup>b</sup>

	EDU18 - PRO18
Z	-4.220 <sup>a</sup>
Asymp.	.000

-----  
 Sig. (2-  
 tailed)  
 -----

a Based on positive ranks.

b Wilcoxon Signed Ranks Test

### Question pro19 and edu19

#### Statistics

		PRO19	EDU19
N	Valid	125	99
	Missing	0	26
Mean		3.6800	3.6970
Std. Error of Mean		.08546	.14174
Std. Deviation		.95546	1.41027
Skewness		-.275	-.914
Std. Error of Skewness		.217	.243
Minimum		1.00	1.00
Maximum		5.00	5.00

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2- sided)
Pearson Chi- Square	15.355 <sup>a</sup>	16	.499
Likelihood Ratio	17.618	16	.347
Linear- by-Linear Association	.491	1	.484
N of Valid Cases	99		

a 15 cells (60.0%) have expected count less than 5. The minimum expected count is .02.

#### Symmetric Measures

		Value	Asymp. Std. Error <sup>a</sup>	Approx. T <sup>b</sup>	Approx. Sig.
Ordinal	Kendall's	-.089	.096	-.929	.353

---

by	tau-b
Ordinal	
N of	99
Valid	
Cases	

---

a Not assuming the null hypothesis.

b Using the asymptotic standard error assuming the null hypothesis.

#### Test Statistics<sup>b</sup>

---

	EDU19 -
	PRO19
Z	-.783 <sup>a</sup>
Asymp.	.434
Sig. (2-	
tailed)	

---

a Based on negative ranks.

b Wilcoxon Signed Ranks Test

### Questions pro20 and edu20

#### Statistics

---

		PRO20	EDU20
N	Valid	125	99
	Missing	0	26
Mean		3.0320	4.3030
Std. Error		.07356	.09132
of Mean			
Std.		.82243	.90863
Deviation			
Skewness		.294	-1.476
Std. Error		.217	.243
of			
Skewness			
Minimum		1.00	1.00
Maximum		5.00	5.00

---

#### Chi-Square Tests

---

	Value	df	Asymp. Sig. (2- sided)
Pearson	14.883 <sup>a</sup>	16	.533
Chi-			
Square			
Likelihood Ratio	13.554	16	.632
Linear-	.001	1	.976

---

by-Linear  
Associati  
on  
N of 99  
Valid  
Cases

a 18 cells (72.0%) have expected count less than 5. The minimum expected count is .02.

### Symmetric Measures

		Value	Asymp. Std. Error <sup>a</sup>	Approx. T <sup>b</sup>	Approx. Sig.
Ordinal by Ordinal	Kendall's tau-b	-.028	.094	-.298	.765
N of Valid Cases		99			

a Not assuming the null hypothesis.

b Using the asymptotic standard error assuming the null hypothesis.

### Test Statistics<sup>b</sup>

	EDU20 - PRO20
Z	-7.124 <sup>a</sup>
Asymp. Sig. (2- tailed)	.000

a Based on negative ranks.

b Wilcoxon Signed Ranks Test

### Questions pro21 and edu21

#### Statistics

	PRO21	EDU21
N	125	99
Valid Missing	0	26
Mean	3.4480	3.4444
Std. Error of Mean	.08832	.16194
Std. Deviation	.98747	1.61133
Skewness	-.236	-.562
Std. Error of Skewness	.217	.243

Minimum	1.00	1.00
Maximum	5.00	5.00

#### Chi-Square Tests

	Value	df	Asymp. Sig. (2- sided)
Pearson Chi- Square	20.343 <sup>a</sup>	16	.205
Likelihood Ratio	21.934	16	.145
Linear- by-Linear Association	.033	1	.856
N of Valid Cases	99		

a 18 cells (72.0%) have expected count less than 5. The minimum expected count is .06.

#### Symmetric Measures

	Value	Asymp. Std. Error <sup>a</sup>	Approx. T <sup>b</sup>	Approx. Sig.
Ordinal by Ordinal tau-b	.057	.089	.645	.519
N of Valid Cases	99			

a Not assuming the null hypothesis.

b Using the asymptotic standard error assuming the null hypothesis.

#### Test Statistics<sup>b</sup>

	EDU21 - PRO21
Z	-.089 <sup>a</sup>
Asymp. Sig. (2- tailed)	.929

a Based on negative ranks.

b Wilcoxon Signed Ranks Test

#### Questions pro22 and edu22



## Statistics

		PRO22	EDU22
N	Valid	125	99
	Missing	0	26
Mean		3.7440	3.5556
Std. Error of Mean		.08644	.16696
Std. Deviation		.96640	1.66122
Skewness		-.227	-.747
Std. Error of Skewness		.217	.243
Minimum		1.00	1.00
Maximum		5.00	5.00

## Chi-Square Tests

	Value	df	Asymp. Sig. (2-sided)
Pearson Chi-Square	7.994 <sup>a</sup>	16	.949
Likelihood Ratio	8.674	16	.926
Linear-by-Linear Association	.034	1	.853
N of Valid Cases	99		

a. 16 cells (64.0%) have expected count less than 5. The minimum expected count is .01.

## Symmetric Measures

		Value	Asymp. Std. Error <sup>a</sup>	Approx. T <sup>b</sup>	Approx. Sig.
Ordinal by Ordinal	Kendall's tau-b	-.026	.090	-.285	.776
N of Valid Cases		99			

a. Not assuming the null hypothesis.

b. Using the asymptotic standard error assuming the null hypothesis.

Test Statistics<sup>b</sup>

	EDU22 - PRO22
Z	-.777 <sup>a</sup>
Asymp. Sig. (2- tailed)	.437

a Based on positive ranks.

b Wilcoxon Signed Ranks Test

## Questions pro23 and edu23

## Statistics

		PRO23	EDU23
N	Valid	125	99
	Missing	0	26
Mean		3.9040	3.6768
Std. Error of Mean Std. Deviation		.07571	.13908
Skewness		.84647	1.38379
Std. Error of Skewness		-.058	-.765
Minimum		.217	.243
Maximum		2.00	1.00
		5.00	5.00

## Chi-Square Tests

	Value	df	Asymp. Sig. (2- sided)
Pearson Chi- Square	7.893 <sup>a</sup>	12	.793
Likelihood Ratio	7.473	12	.825
Linear- by-Linear Association	.065	1	.798
N of Valid Cases	99		

a 11 cells (55.0%) have expected count less than 5. The minimum expected count is .02.

## Symmetric Measures

		Value	Asymp. Std. Error <sup>a</sup>	Approx. T <sup>b</sup>	Approx. Sig.
Ordinal	Kendall's	-.045	.085	-.533	.594
by	tau-b				
Ordinal					
N of		99			
Valid					
Cases					

a Not assuming the null hypothesis.

b Using the asymptotic standard error assuming the null hypothesis.

Test Statistics<sup>b</sup>

		EDU23 - PRO23
Z		-.839 <sup>a</sup>
Asymp. Sig. (2- tailed)		.402

a Based on positive ranks.

b Wilcoxon Signed Ranks Test

## Appendix R

### Raw Data

## Information Security Professionals Raw Data

p 1	p 2	p 3	p 4	p 5	p 6	p 7	p 8	p 9	p 10	p 11	p 12	p 13	p 14	p 15	p 16	p 17	p 18	p 19	p 20	p 21	p 22	p 23
5	5	1	4	3	3	4	3	1	1	3	1	4	4	1	4	1	3	2	2	1	3	3
4	4	4	4	4	3	4	4	4	3	4	4	4	4	4	4	4	4	2	3	4	4	4
2	4	4	4	5	2	4	3	3	3	5	3	3	4	2	4	4	4	3	3	4	4	4
4	4	4	4	3	3	3	3	3	3	4	3	2	4	3	4	3	4	3	3	3	4	3
5	5	5	4	5	5	4	4	5	3	4	4	4	5	3	5	4	4	3	3	3	4	4
5	4	4	5	4	5	4	4	4	3	3	3	4	5	4	4	4	5	3	3	3	3	4
5	5	5	4	4	4	4	4	4	4	3	3	3	4	3	4	4	3	3	3	3	2	3
4	4	4	4	4	3	4	4	4	2	3	2	2	4	3	4	4	4	3	3	4	5	4
4	4	4	4	4	4	5	5	3	2	1	1	4	3	4	4	4	4	2	2	3	3	3
5	5	4	5	5	4	4	3	3	2	3	3	4	5	4	4	4	3	3	2	2	3	3
5	5	5	5	5	5	5	5	5	5	5	4	5	5	5	4	5	5	4	4	5	5	5
5	5	4	5	4	4	5	4	4	3	4	4	5	5	5	4	4	4	4	2	4	5	4
4	5	2	5	5	4	5	2	3	2	4	4	5	4	4	4	4	3	1	1	1	5	5
5	5	1	4	3	3	4	3	1	1	3	1	4	4	1	4	1	3	2	2	1	3	3
3	4	4	4	5	4	4	3	4	2	4	2	4	5	4	4	5	5	4	2	2	2	4
4	4	5	4	5	5	3	3	3	2	2	2	4	5	4	5	5	4	5	2	4	5	3
5	5	3	3	5	4	3	2	4	3	5	5	5	5	4	3	3	4	4	2	2	3	3
4	4	4	4	4	4	5	3	3	3	4	4	5	5	5	5	4	4	4	4	4	5	4
5	5	5	5	5	5	5	5	3	3	5	4	5	5	5	5	5	5	4	4	4	3	3
5	5	5	4	5	3	3	5	4	4	5	2	4	5	5	5	5	5	5	3	5	4	5
3	4	4	4	5	5	4	4	4	4	5	3	3	3	3	5	4	5	3	3	4	5	4
5	5	5	5	5	4	4	4	5	4	4	4	4	4	4	4	4	5	5	5	5	5	5
5	5	5	5	5	5	5	2	4	3	5	3	3	4	3	4	5	5	3	3	3	5	5
5	5	3	4	4	4	4	4	4	5	4	5	4	4	3	4	4	4	3	3	3	3	3
5	5	4	4	5	4	5	4	5	3	4	3	4	5	4	4	4	5	5	3	3	3	4
5	5	5	4	4	4	4	4	4	4	3	3	3	4	3	4	4	3	3	3	3	2	3
5	5	4	4	3	3	3	3	4	3	3	3	3	4	3	3	4	3	3	3	4	3	3
4	4	4	4	5	4	3	3	4	4	4	2	5	4	4	4	4	4	4	5	4	5	5
5	5	4	4	4	5	5	2	5	4	3	3	3	4	3	4	4	3	3	4	4	4	4
5	5	4	5	4	4	5	4	4	3	4	4	5	5	5	4	4	4	4	2	4	5	4
5	5	5	4	5	5	5	4	5	5	4	4	4	5	5	4	4	5	5	4	5	5	5
5	5	3	5	5	5	4	4	5	5	4	4	4	3	3	4	3	4	4	3	4	3	3

5 5 5 5 5 5 5 5 5 5 5 4 5 5 5 4 5 5 4 4 5 5 5  
 5 5 4 4 3 3 3 3 4 3 3 3 3 4 3 3 4 3 3 3 4 3 3  
 5 5 5 5 5 5 5 5 5 5 5 4 5 5 5 4 5 5 4 4 5 5 5  
 4 5 3 4 5 5 5 5 4 3 4 3 3 4 3 4 4 4 3 2 3 5 3  
 5 4 5 4 5 5 4 4 4 4 4 4 4 4 4 4 4 4 3 3 3 5 5  
 5 4 4 5 5 4 4 3 4 4 3 3 4 4 3 4 5 5 4 3 3 3 4  
 5 5 5 4 5 5 5 5 5 5 3 3 4 4 3 5 4 5 5 3 3 3 5  
 4 4 4 4 4 4 4 3 3 3 4 3 4 4 4 4 3 3 2 2 2 3 3  
 5 5 5 4 5 5 5 5 5 4 4 4 5 4 5 5 5 4 4 4 4 4 5  
 5 5 4 4 5 4 5 4 5 3 4 3 4 5 4 4 4 5 5 3 3 3 4  
 5 5 2 4 5 3 5 5 5 3 3 3 5 4 3 4 3 5 5 3 3 3 5  
 5 5 5 4 5 5 4 4 5 4 4 4 4 3 3 3 4 4 5 3 3 4 4  
 5 4 4 5 4 5 4 4 4 3 3 3 4 5 4 4 4 5 3 3 3 3 4  
 5 5 3 4 4 4 4 4 4 5 4 5 4 4 3 4 4 4 3 3 3 3 3  
 4 4 4 4 5 5 5 5 4 4 5 5 5 5 5 5 5 5 5 5 5 5  
 4 5 4 4 5 3 5 3 2 2 3 2 3 4 3 4 5 5 4 4 3 4 4  
 4 4 4 4 4 4 4 3 3 3 4 3 4 4 4 4 3 3 2 2 2 3 3  
 5 5 3 5 5 5 4 4 5 5 4 4 4 3 3 4 3 4 4 3 4 3 3  
 4 4 4 4 3 3 3 3 3 3 4 3 2 4 3 4 3 4 3 3 3 4 3  
 5 5 4 4 3 3 3 3 4 3 3 3 3 4 3 3 4 3 3 3 4 3 3  
 4 4 4 4 4 2 4 3 4 2 4 4 4 4 3 3 4 2 2 2 2 3 4  
 5 5 5 4 5 5 4 4 5 3 4 4 4 5 3 5 4 4 3 3 3 4 4  
 5 4 4 5 5 4 4 3 4 4 3 3 4 4 3 4 5 5 4 3 3 3 4  
 5 5 5 4 5 5 5 5 5 4 3 3 5 3 5 5 5 5 5 5 5 5  
 4 4 4 4 3 3 3 3 3 3 4 3 2 4 3 4 3 4 3 3 3 4 3  
 5 5 3 4 4 4 4 4 4 4 5 4 5 4 4 3 4 4 4 3 3 3 3  
 5 5 3 3 5 5 5 5 5 3 3 5 5 5 4 5 3 4 3 2 2 3 4  
 5 5 4 4 4 4 4 4 4 4 4 2 2 3 4 3 5 5 5 3 5 4 5  
 4 4 4 4 4 3 4 3 4 4 4 4 4 3 4 2 4 4 4 4 2 2 1 4  
 4 4 5 4 5 5 3 3 3 2 2 2 4 5 4 5 5 4 5 2 4 5 3  
 5 5 3 5 5 5 4 4 5 5 4 4 4 3 3 4 3 4 4 3 4 3 3  
 5 5 5 4 5 5 5 4 5 5 4 4 4 5 5 4 4 5 5 4 5 5 5  
 5 5 5 4 5 4 5 5 5 4 4 4 5 2 4 5 5 5 5 4 2 5 5  
 3 3 4 4 4 3 3 2 2 2 3 2 3 3 4 3 4 3 3 3 2 2  
 5 5 5 4 5 4 4 5 5 5 4 4 5 4 4 4 5 4 4 3 4 4 3  
 5 5 3 4 4 4 4 4 4 5 4 5 4 4 3 4 4 4 3 3 3 3 3

5 5 5 5 5 5 5 5 5 5 5 4 5 5 5 4 5 5 4 4 5 5 5  
4 4 4 4 3 3 3 3 3 3 4 3 2 4 3 4 3 3 3 3 4 3  
5 5 5 4 4 4 4 3 4 4 3 4 3 3 5 5 5 3 3 4 3 5  
4 4 4 4 3 3 3 3 3 3 4 3 2 4 3 4 3 3 3 3 4 3  
5 5 3 5 5 5 4 4 5 5 4 4 4 3 3 4 3 4 4 3 4 3 3  
4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 3 3 4 4  
4 4 2 4 3 2 4 5 4 4 4 4 4 5 4 4 3 4 2 4 3 5 4  
4 4 5 3 3 4 5 4 4 2 2 2 3 4 4 5 5 3 3 2 4 3 3  
5 5 4 5 4 5 5 4 4 5 5 1 4 3 5 4 4 4 3 3 5 4 4  
5 5 4 5 4 4 5 4 4 3 4 4 5 5 5 4 4 4 4 2 4 5 4  
5 5 5 4 4 4 4 4 5 4 3 2 5 5 5 5 5 5 2 2 4 3  
5 5 5 4 4 4 4 3 4 4 3 4 3 3 3 5 5 5 3 3 4 3 5  
4 4 2 4 3 2 4 5 4 4 4 4 4 5 4 4 3 4 2 4 3 5 4  
5 5 5 4 4 4 4 3 4 4 3 4 3 3 3 5 5 5 3 3 4 3 5  
5 4 4 5 4 5 4 4 4 3 3 3 4 5 4 4 4 5 3 3 3 3 4  
5 5 5 5 5 5 5 5 5 4 5 5 5 5 5 5 5 5 5 5 5 5  
4 5 4 4 5 3 5 3 2 2 3 2 3 4 3 4 5 5 4 4 3 4 4  
5 5 4 4 5 4 3 3 2 2 4 4 4 4 3 4 4 4 4 3 4 4 3  
4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 4 3 3 4 4  
4 4 4 4 5 4 3 3 3 2 4 4 5 5 4 4 4 4 3 4 4 4 4  
5 5 5 3 4 4 4 4 5 3 3 3 4 4 3 4 4 3 3 3 3 4 3  
5 5 4 4 3 3 3 3 4 3 3 3 3 4 3 3 4 3 3 3 4 3 3  
5 5 5 4 4 4 4 4 4 4 3 3 3 4 3 4 4 3 3 3 2 3  
5 5 3 4 4 4 3 3 4 3 3 2 4 4 3 3 3 4 4 3 4 3 4  
5 5 5 5 5 4 5 5 5 4 4 4 5 4 4 4 5 4 4 3 3 3 4  
5 4 4 5 5 4 4 3 4 4 3 3 4 4 3 4 5 5 4 3 3 3 4  
5 5 2 4 5 3 5 5 5 3 3 3 5 4 3 4 3 5 5 3 3 3 5  
5 5 4 4 4 2 3 4 4 4 4 4 4 4 4 4 4 4 3 3 3 4  
5 5 5 4 4 4 4 3 4 4 3 4 3 3 3 5 5 5 3 3 4 3 5  
5 5 4 4 3 3 3 3 4 3 3 3 3 4 3 3 4 3 3 3 4 3 3  
5 5 5 4 5 4 4 5 5 5 4 4 5 4 4 4 5 4 4 3 4 4 3  
5 5 3 4 4 4 4 4 4 4 5 4 5 4 4 3 4 4 4 3 3 3 3  
4 4 4 4 5 4 4 4 4 4 2 2 4 4 3 4 4 4 3 3 4 3 5  
3 4 4 4 5 4 4 3 4 2 4 2 4 5 4 4 5 5 4 2 2 2 4  
5 5 1 3 3 4 5 4 5 1 4 1 4 4 4 3 1 4 5 1 3 4 5  
5 5 5 5 5 4 5 5 5 3 4 4 4 4 4 5 5 5 5 3 5 5 5

5 5 2 4 5 3 5 5 5 3 3 3 5 4 3 4 3 5 5 3 3 3 5  
4 5 5 4 5 3 5 5 3 2 4 2 4 5 2 4 5 3 2 3 5 5 4  
5 5 5 4 5 4 4 5 5 5 4 4 5 4 4 4 5 4 4 3 4 4 3  
5 5 4 4 4 4 4 4 4 4 2 2 3 4 3 5 5 5 5 3 5 4 5  
5 5 5 4 5 5 4 4 5 3 4 4 4 5 3 5 4 4 3 3 3 4 4  
5 5 3 5 5 5 4 4 5 5 4 4 4 3 3 4 3 4 4 3 4 3 3  
5 5 4 4 5 4 5 4 5 3 4 3 4 5 4 4 4 5 5 3 3 3 4  
5 5 5 4 5 4 4 5 5 5 4 4 5 4 4 4 5 4 4 3 4 4 3  
5 5 4 4 4 5 5 4 4 2 5 3 4 3 3 5 4 5 5 4 5 4 5  
4 4 4 4 5 4 3 3 4 4 4 2 5 4 4 4 4 4 4 5 4 5 5  
5 5 5 5 4 5 5 4 4 4 4 3 4 4 3 4 4 4 5 3 3 5 2  
5 4 4 4 5 4 5 5 4 4 3 3 5 5 3 4 4 5 5 4 4 4 5  
5 5 4 4 5 5 4 5 2 2 5 5 5 4 4 4 4 4 3 4 5 4  
3 3 2 3 4 3 4 4 3 2 3 2 3 4 2 4 2 4 3 3 4 4 4  
4 4 4 4 4 3 4 3 4 4 4 4 3 4 2 4 4 4 4 2 2 1 4  
4 4 4 4 4 3 4 4 4 3 4 4 4 4 4 4 4 4 4 2 3 4 4  
5 5 5 4 5 5 5 5 5 5 5 5 5 4 5 5 5 5 5 5 5 5 5  
5 5 5 4 5 5 5 4 5 5 4 4 4 5 5 4 4 5 5 4 5 5 5  
4 5 4 4 5 3 5 3 2 2 3 2 3 4 3 4 5 5 4 4 3 4 4  
3 4 2 4 3 3 3 3 2 2 3 2 3 4 2 3 2 2 2 2 2 3 2  
4 5 2 5 5 4 5 2 3 2 4 4 5 4 4 4 4 3 1 1 1 5 5





3 3 3 4 3 1 3 3 3 3 3 1 3 3 3 3 3 3 3 1 1 3  
 4 4 2 4 4 2 3 1 3 2 4 2 3 2 2 2 2 3 1 2 1 1 1  
 4 4 4 3 3 2 4 3 3 3 4 4 4 5 4 3 5 3 2 5 4 5 5  
 3 5 5 3 5 5 5 5 3 1 5 1 5 5 4 5 5 5 5 5 5 5  
 3 3 3 4 3 1 3 3 3 3 3 1 3 3 3 3 3 3 3 3 1 1 3  
 3 3 3 4 3 1 3 3 3 3 3 1 3 3 3 3 3 3 3 3 1 1 3  
 1 3 1 2 2 1 4 1 3 2 2 1 1 1 1 1 1 1 1 4 1 3 1  
 3 3 3 4 3 1 3 3 3 3 3 1 3 3 3 3 3 3 3 3 1 1 3  
 4 4 4 3 4 3 5 4 4 3 5 3 5 4 3 3 5 3 4 4 4 5 4  
 1 1 4 1 2 1 1 3 4 3 1 2 1 1 1 1 4 1 1 4 1 1 1  
 4 4 4 3 4 3 5 4 4 3 5 3 5 4 3 3 5 3 4 4 4 5 4  
 1 1 4 2 2 1 2 3 4 3 1 2 1 1 1 1 4 1 1 4 1 1 1  
 4 4 4 3 4 3 5 4 4 3 5 3 5 4 3 3 5 3 4 4 4 5 4  
 1 1 4 2 2 1 2 3 4 3 1 2 1 1 1 1 4 1 1 4 1 1 1  
 4 4 4 3 4 3 5 4 4 3 5 3 5 4 3 3 5 3 4 4 4 5 4  
 4 4 4 3 4 3 5 4 4 3 5 3 5 4 3 3 5 3 4 4 4 5 4  
 1 1 4 1 2 2 2 3 4 3 1 2 1 2 1 1 4 1 1 4 2 1 2  
 4 4 4 3 4 3 5 4 4 3 5 3 5 4 3 3 5 3 4 4 4 5 4  
 1 1 4 1 2 1 1 3 4 3 1 2 1 1 1 1 4 1 1 4 1 1 1  
 4 4 4 3 4 3 5 4 4 3 5 3 5 4 3 3 5 3 4 4 4 5 4  
 1 1 4 2 2 1 2 3 4 3 1 2 1 1 1 1 4 1 1 4 1 1 1  
 4 4 4 3 4 3 5 4 4 3 5 3 5 4 3 3 5 3 4 4 4 5 4  
 1 1 4 2 2 1 2 3 4 3 1 2 1 1 1 1 4 1 1 4 1 1 1  
 4 4 4 3 4 3 5 4 4 3 5 3 5 4 3 3 5 3 4 4 4 5 4  
 4 4 4 3 4 3 5 4 4 3 5 3 5 4 3 3 5 3 4 4 4 5 4  
 1 1 4 2 2 1 2 3 4 3 1 2 1 1 1 1 4 1 1 4 1 1 1  
 4 4 4 3 4 3 5 4 4 3 5 3 5 4 3 3 5 3 4 4 4 5 4  
 1 1 4 2 2 1 2 3 4 3 1 2 1 1 1 1 4 1 1 4 1 1 1  
 4 4 4 3 4 3 5 4 4 3 5 3 5 4 3 3 5 3 4 4 4 5 4  
 4 4 4 3 4 3 5 4 4 3 5 3 5 4 3 3 5 3 4 4 4 5 4  
 4 4 4 3 4 3 5 4 4 3 5 3 5 4 3 3 5 3 4 4 4 5 4  
 1 1 4 2 2 1 2 3 4 3 1 2 1 1 1 1 4 1 1 4 1 1 1  
 4 4 4 3 4 3 5 4 4 3 5 3 5 4 3 3 5 3 4 4 4 5 4  
 4 4 4 3 4 3 5 4 4 3 5 3 5 4 3 3 5 3 4 4 4 5 4  
 4 4 4 3 4 3 5 4 4 3 5 3 5 4 3 3 5 3 4 4 4 5 4  
 3 4 5 4 4 3 4 4 5 3 4 4 4 5 3 3 5 3 4 5 3 4 3



## Reference List

- Alreck, P. & Settle, R. (1995). *The Survey Research Handbook*. New York: McGraw-Hill.
- Bartlett, J. E., Kotrlik, J. W., & Higgins, C. C. (2001). Organizational research: Determining appropriate sample size in survey research. *Information Technology, Learning, and Performance Journal*, 19, 43-50.
- Benamati, J. (1999). An empirical study of IT management and rapid IT change. *Proceedings of the 1999 ACM SIGCPR Conference on Computer Personnel Research*. (p.144) New Orleans: ACM.
- Bishop, M. (1997). The state of INFOSEC education in academia: Present and future directions. *Proceedings of the National Colloquium on Information Security Education*. (p.15) Linthicum, National Colloquium.
- Bishop, M. (2000). Academia and education in information security: Four years later. *Proceedings of the National Colloquium on Information System Security*. (p.30) Washington, National Colloquium.
- Blumenthal, M. S. (1999). The politics and policies of enhancing trustworthiness for information systems. *Communications Law & Policy*, 4, 512.
- Centers of Academic Excellence in Information Assurance Education. Retrieved December 2, 2002 from <http://www.nsa.gov/isso/programs/coeiae/measure.html>.
- Chin, S., Irvine, C., & Frincke, D. (1997). *An information security education initiative for engineering and computer science*. Paper presented at Syracuse University, Syracuse, NY.
- CISSP Certification Common Body of Knowledge Study Guide* (2000). Available from The International Information Systems Security Certification Consortium, Shrewsbury, MA.
- Dark, M. & Davis, J. (2002). *Report on information assurance curriculum development*. Paper presented at the meeting of the NCISSE, Washington, DC.

- Desai, M. S. & Von Der Embse, T. (2001). A synergistic strategy for MIS curriculum development: Response to rapidly advancing information technology. *College Student Journal*, 35, 552.
- Dhillon, G. & Blackhouse, J. (2000). Information systems security management in the new millennium. *Communications of the ACM*, 43, 125-128.
- Dugan, S. & Prencipe, L. W. (2001). Certifiability secured. *Infoworld*, 23, 36.
- Feustel, E. & Mayfield, T. (1998). The DGSA: Unmet information security challenges for operating systems designer. *ACM SIGOPS Operating Systems Review*, 32, 3.
- Golshani, F., Panchanathan, S., Friesen, O., Park, Y. C. & Song, J. J. (2001). A comprehensive curriculum for IT education and workforce development: An engineering approach. *Proceedings of the Thirty Second SIGCSE Technical Symposium on Computing*, (p.238) Charlotte: CSE.
- Gordon, L. & Loeb, M. (2002). The economics of information security investment. *ACM Transactions on Information and Systems Security*, 5, 438.
- Grimaila, M. R. & Kim, I. (2002). An undergraduate business information security course and laboratory. *Journal of Information Systems Education*, 13, 189-195.
- Hazari, S. (2002). Reengineering an information security course for business management focus. *Journal of Information Systems Education*, 13, 23.
- Information assurance curriculum and certification: State of the practice* (1999)  
Retrieved August 2002 from  
<http://www.sei.edu/publications/documents/99.reports>.
- Irvine, C. E. (1996). Goals for computer security education. *Proceedings of IEEE Symposium on Security and Privacy*. (p.24) Oakland: IEEE.
- Irvine, C., Warren, D., & Clark, P. (1997). The NPS CISR graduate program in InfoSec: Six years of experience. *Proceedings of the 20th National Information Security Conference*. (p.22) Baltimore: NIST.
- IT Risk Management Series: Executive Guide to Internet Security*. (1999). Retrieved March 2000 from <http://www.ey.com>.
- Kim, S. & Choi, M. (2002). Educational requirement analysis for information security professionals in Korea. *Journal of Information Systems Education*, 13, 237.
- Krutz, R. L. & Vines, R. (2001). *The CISSP Prep Guide*. New York: Wiley.
- Lightfoot, J. M. (1999). Fad versus fundamentals: The dilemma for information systems curriculum design. *Journal of Education for Business*, 75(1), 43-51.

- Litwin, M. S. (1995). *How to Measure Survey Reliability and Validity*. Thousand Oaks, CA: Sage.
- Logan, P. Y. (2002). Creating an undergraduate information security emphasis within information technology. *Journal of Information Systems Education*, 13, 177-182.
- Longmore-Etheridge, A. (2000). Long's day journey into knowledge. *Security Management*, 44, 61-64.
- McCollum, K. (2000). Colleges struggle to train experts in protecting computer systems. *The Chronicle of Higher Education*, 46, 61.
- National Security Agency, *NSTISSI*, (1990). Washington DC, U.S. Government Printing Office.
- National Security Agency, *Critical infrastructure protection in the information age*, (2001). Washington, DC, U.S. Government Printing Office.
- Piazza, P. (2001). Holistic infosec institute. *Security Management*, 45, 2.
- Prahalad, C. & Krishnan, M. (2002). The dynamic synchronization of strategy and information technology. *MIT Sloan Management Review*, 43, 24.
- Reynolds, W. (1998). *Report of the 1998 Annual Meeting for the National Colloquium for Information Systems Security Education*. Retrieved, December 2002, from <http://www.jmu.edu>.
- Rose, G., Khoo, H., & Straub, D. (1999). Current technologies impediments to business-to-consumer electronic commerce. *Communications of the ACM*, 1, 1.
- Rosenthal, D. (1999). Intrusion detection technology: Leveraging the organization's security posture. *Information Systems Management*, 19, 35.
- Saita, A. (2002). Bridging the gap. *Information Security*, 5, 38.
- Schneider, F. (2000). Enforceable security policies. *ACM Transactions on Information and Systems Security*, 3, 30.
- Sumner, M. & Werner, K. (1997). On-line ethics: A comparison of the attitudes of freshmen, MIS majors, and practitioners. *Proceedings of the 1997 Conference on Computer Personnel Research*. (p.35) San Francisco: ACM.
- The International Information Security Foundation (I<sup>2</sup>SF) (1999). Retrieved December 2002 from <http://web.mit.edu/security/www/gassp1.html#background>.
- The Joint Task Force on Computing Curricula, IEEE Computer Society, Association for Computing Machinery* (2001). Association for Computing Machinery, Inc.

- Torkzadeh, G. & Doll, J. (1999). The development of a tool for measuring the perceived impact of information technology on work. *Omega*, 27, 327.
- Yang, T. A. (2001). Computer security and impact on computer science education. *Proceedings of the Sixth Annual CCSC Northeastern Conference*, (233) Middlebury, VT: ACM.
- Yasinsac, A. (1999). Information security curricula in computer science department: Theory and practice: Florida State University. Unpublished manuscript, Florida State University, Tallahassee, FL.