AN ANALYSIS OF THE OPINIONS OF DATA PROCESSING

MANAGEMENT ASSOCIATION MEMBERS CONCERNING

DATA SECURITY CURRICULA IN HIGHER

EDUCATION INSTITUTIONS

By

KAREN ANNE FORCHT

Bachelor of Science
Bowling Green State University
Bowling Green, Ohio
1970

Master of Science
East Texas State University
Commerce, Texas
1974

Submitted to the Faculty of the Graduate College
of the Oklahoma State University
in partial fulfillment of the requirements
for the Degree of
DOCTOR OF EDUCATION
December, 1984

AN ANALYSIS OF THE OPINIONS OF DATA PROCESSING
MANAGEMENT ASSOCIATION MEMBERS CONCERNING
DATA SECURITY CURRICULA IN HIGHER
EDUCATION INSTITUTIONS

Thesis Approved:

Thesis Adviser

Norman N. Durham
Dean of the Graduate College

ACKNOWLEDGMENTS

My sincere and heartfelt appreciation is extended to the members of my dissertation committee: to Dr. Herbert Jelley, Chairperson, a sincere thank you for his unfailing encouragement, suggestions, guidance, and for not allowing me to make any "big" mistakes; to Dr. Jeretta Horn, Thesis Adviser, for her expertise in the technical aspects of computer security and never-ending patience; to Dr. Dennis Mott, for his assistance when "brainstorming" topics and invaluable support as a very competent and cooperative department chairperson; and to Dr. Robert Kamm, for his invaluable input and continuing, after numerous dissertations, to "take pride in the novice".

A special thank you to Mr. Davis Sellers for his assistance in developing the pilot study mailing list; to Mr. Gary Clure and Miss Barbara Howell for their statistical expertise; to the very capable typists at Velda Davis' TOP Services Unlimited for their expert typing of the dissertation; and to all the DPMA members who responded to the questionnaire, a debt of professional gratitude is extended.

For their generous financial assistance, use of their research facilities, and willingness to aid with the questionnaire design, I am indebted to the office of Business and Economic Research of the College of Business Administration.

Acknowledging that persons outside the normal academic circles also play a very vital role, I would like to thank three very good friends, Joan Roderick, Debra Renshaw, and Tom Gibson who were always there with words of encouragement.

To my parents, John and Rhea Bishop, I would like to thank for showing me many years ago that "hard work" does yield its own reward.

And most of all, I would like to thank the two <u>special</u> young ladies who provided the impetus for this pursuit, my daughters, Nicole and Michelle. Their quiet confidence provided the constant motivation that made completion attainable.

TABLE OF CONTENTS

Chapter	Page

LIST OF TABLES

Table		Page

Table		Page

Table Page

Table		Page
LXXX.	Comparison of Whether Computer Center Employees Should Possess Knowledge of Computer Security and Number of People in Respondent's Computer Center Directly Responsible for Computer Security	281
LXXXI.	Comparison of Whether Computer Center Employees Should Possess Knowledge of Computer Security and Respondent's Present Position	282
LXXXII.	Comparison of Whether Computer Center Employees Should Possess Knowledge of Computer Security and Respondent's Length of Time in Present Position	283
LXXXIII.	Comparison of Whether Computer Center Employees Should Possess Knowledge of Computer Security and Respondent's Highest Educational Level	284
LXXXIV.	Comparison of Whether Computer Center Employees Should Possess Knowledge of Computer Security and Respondent's Major Area of Study	285
LXXXV.	Comparison of Whether Computer Center Employees Should Possess Knowledge of Computer Security and Number of Employees Directly Supervised by Respondent	286
LXXXVI.	Comparison of Whether Computer Center Employees Should Possess Knowledge of Computer Security and Respondent's Membership in Data Processing Professional Organizations	287
LXXXVII.	Comparison of Methods Respondents Feel Would Best Develop Computer Security Knowledge and Number of Employees in Respondents Computer Center	288
LXXXVIII.	Comparison of Methods Respondents Feel Would Best Develop Computer Security Knowledge and Whether Respondent's Computer Center has a Designated Person Directly Responsible for Computer Security	289
LXXXIX.	Comparison of Methods Respondents Feel Would Best Develop Computer Security Knowledge and the Number of People in Respondent's Computer Center Directly Responsible for Computer Security	290
LXXXX.	Comparison of Methods Respondents Would Best Develop Computer Security Knowledge and the Respondent's Present Position	291

Table Page

LIST OF FIGURES

CHAPTER I

STATEMENT OF THE PROBLEM

Introduction

The past decade has seen the rapid development and proliferation of computers in organizations of all sizes and types. Often, as this growth proceeded, security was not considered in the system design stages. Except where security has been very obviously of major importance (e.g., in banking systems or top secret military or defense research projects) it has often been conveniently ignored by designers of computer systems. According to Farr (1972, p. 16), "This attitude may well have resulted from lack of understanding by company management of the functioning of their computer systems and their peculiar vulnerability to novel forms of fraud and malicious interference." However, recently it has been recognized that computing systems are easily compromised. This is especially true since most security systems have evolved on an ad hoc basis with "patches" made in elements of the system to thwart any perceived weaknesses.

The growth of the interest in data security stems from two main directions--awareness by companies that data stored in computer systems is vulnerable, and concern on the part of certain individuals and social bodies about intrusions into individual privacy.

The problem of data security becomes even more paramount and complex as our present office environment becomes increasingly automated.

Prince (1980) in his article entitled, "What It Will Take to Manage in the '80's," said,

> The office environment will consist of such things as advanced word processing systems, minicomputers, reprographics, micrographics, teleconferences, video conferencing, and telecommunications--all interrelated through integrated networks (p. 34).

Managers will have to be versatile and innovative in "juggling" the demands of technology, information, and people. The threats to security become even more numerous as systems increase in complexity.

In order for office personnel to be prepared for such roles, colleges and universities must begin to recognize the urgent need to enhance their curricula by including data security topics so that college graduates entering the business environment are cognizant of the importance of data security.

Society's Dependence on Information Systems

As society moves toward electronic mail and other large extensively used information systems, likely new issues and topics will need to be considered regarding how public policy can help balance the risks versus the benefits society may encounter. Other issues to be considered along with these risk factors are:

- Retaining the option to end dependence on a particular system (avoiding becoming "locked in").
- Providing alternatives for those who prefer not to use electronic services.

Gibbons (1981, p. 9) states that "Research on the risks of system failure is needed, as is careful attention to how technology can be used to reduce these risks (for example, through distributed data bases and back-up computers)."

Gibbons (1981) cites three problem areas to be considered:

- Constitutional rights--Little legal precedent exists, in many cases, for applying constitutional law to issues raised by computer-based information systems. Areas of constitutional rights that may be affected by information systems include: freedom of speech and press (first amendment), protection against unreasonable search and seizure (fourth), protection against self-incrimination and guarantee of due process of law (fifth), right to a trial by impartial jury (sixth), and State guarantees of due process and equal protection of the laws (14th).

- Regulatory boundaries--Evolving computer-based systems are crossing over and blurring traditional regulatory boundaries. Regulatory policy issues are likely to recur with respect to computer- v. communication-based services, electronic interstate branch banking, and electronic mail. As these systems expand geographically and move away from traditional definitions of industry structure, policy issues concerning interstate conflict of laws, Federal-State relationships, and antitrust may also arise.

- Other issues--Four other issue areas were identified as important although not analyzed in great detail: computer crime, transborder data flow, information gap (for those who would be denied access due to technological illiteracy or other reasons), and computer software protection (p. 9).

Issues of Data Security

The areas involved in data security are spread throughout the organization. Data are vulnerable, regardless of where processed. The following are the main areas that will be considered in the focus of this research:

1. Computer fraud
2. Violations of private information
3. Threats to file security
4. Threats to the security of terminals and communications equipment
5. Hardware protection
6. Safeguarding computers

7. Software protection
8. Screening personnel
9. Security audits
10. Physical access control
11. Waste disposal control
12. Privacy of output
13. Fire protection
14. Protection against rioting
15. Backup files
16. Secondary generators and air conditioning
17. Limiting access to the computer room
18. Insurance
19. Telecommunications control
20. Data base protection

The nature of data--along with the necessary resulting security measures--are of two distinct types and is derived from its use. Basically, these two attributes (types) apply: confidentiality and essentiality.

...Confidentiality

If some data concern a private party or person (e.g., client or patient), and if only certain persons are permitted access to it, it possesses a degree of confidentiality.

...Essentiality

If some data have a high degree of importance for a user such that, if lost through unintentional modification or theft it can be recovered only at a high expense, then it possesses a degree of essentiality (Madnick, 1975).

An example of the differentiation between the two types of data could be as follows:

--A proprietary software package possesses high confidentiality because parties outside the vendor-buyer relationships are not allowed examination or use of the package. Essentiality may be very high to the owner, whereas for the buyer, it is rather low (an extra copy can always be obtained). Zip codes have low essentiality because of their public nature and availability (Madnick, 1975).

Common Security Threats and Countermeasures

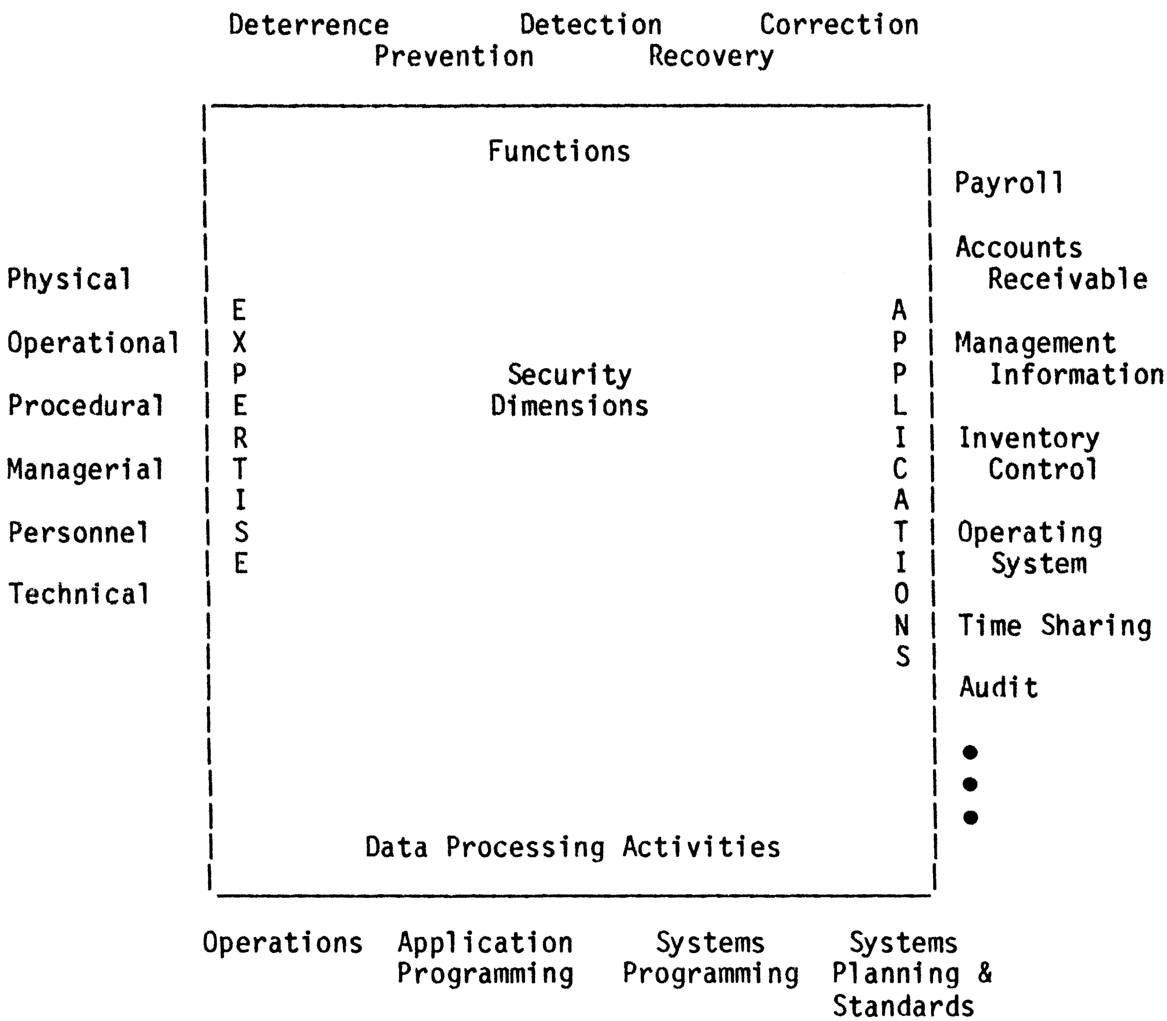
Common threats against data security are computer installation sabotage, accidental system breakdown, fraud, embezzlement, interception errors, disclosure of data, theft, sabotage, or unauthorized copying of data. (See the Dimensions of Computer Security chart, Figure 1, on the following page.) Data security can be created and maintained by some or all of the following elements:

--Technical Protection (automated):

- computer system integrity (such as operating systems, backup power, and fire protection)
- remote access control (such as terminal authorization, and user identification)
- data encoding (encryption)

--Procedural Protection (manual)

- physical access control (such as guards, badges, and locks)
- data handling rules (such as offsite storage and written requisition of storage volumes)
- program modification rules



Source: Parker, 1981, p. 56.

Figure 1. Dimensions of Computer Security

- input/output separation
- input/output controls
- audit

--<u>Personnel Protection</u>

- preemployment screening
- supervision
- division of responsibility (Madnick, 1975).

Parker (1981) cites the following areas as being most vulnerable:

Rank		Percent
1	Physical access to facilities	25
2	Handling of input data	23
3	Logical access to assets	15
4	Business ethics	8
5	Handling of output data	8
6	Access to application programs	7
7	Handling of machine-readable data	7
8	Access to systems programs	3
9	Backup/recovery	2
10	Data communications	1

(p. 134).

In addition, Parker (1981) lists the following assets as being subject to computer security:

Data processing staff
Computer system services
Computer-related facilities
Power, water, and communication utilities
Computer and peripheral equipment
Supplies and data storage media
System and utility computer programs and documentation
Application computer programs and documentation
Data
Safeguards (p. 43).

The sources of threats to computer security encompass virtually all areas in the computer environment. (See Threat Model on the following page, Figure 2.) Measures should be instituted to ensure that all areas are sufficiently covered in order to insure an efficient ongoing security program.

Sources	Motives	Acts	Results	Losses
ADP Employees	Incompetence	Overt	Disclosure	None
Employees	Human failure	Covert	Modification	Monetary
Vendors	Irrational behavior	Descriptive	Destruction	Denial of use/possession
Outsiders	Personal problems	Single event	Use of services	Denial of exclusive use/ possession
Natural forces	Personal gain	Multiple events		Denial of access
	Professional crime	Continuous		Personal values
	Business gain	Physical		Health/life
	Economic advocacy	Logical		Privacy
	Political advocacy	Local/remote access		Other
	Social advocacy	Real-time		
	Religious advocacy	Nonreal-time		
		Collusion		
		Testing		
		Other		

Source: Parker, 1981, p. 136.

Figure 2. Threat Model

Recent Violation

During the summer of 1983, seven youths ranging in age from 15 to 22, in the Milwaukee, Wisconsin area, gained access to computers spread across the United States and Canada. Penetration was made by the 414's (as the group called themselves after the Milwaukee area's telephone area code) into such vital computers as:

1. Memorial Sloan-Kettering Center in New York City
2. A bank in Los Angeles
3. A cement company in Montreal, Canada
4. An unclassified computer at a nuclear weapons laboratory in Los Alamos, New Mexico

According to Elmer-Dewitt (1983),

> The Sloan-Kettering Caper and this summer's hit movie [1983] War Games--the story of a young computer buff who nearly sets off a nuclear war when he accidentally gets into one of the Defense Department's most sensitive machines--have focused attention on a serious question: How to safeguard information stored inside the computer (p. 34).

The potential for fraud is awesome. "The American banking system alone moves more than $400 billion between computers every day" (Elmer-DeWitt, 1983, p. 34). Corporate data banks hold consumer records and business plans worth untold billions. Military computers contain secrets that, if stolen, could threaten United States' security (Elmer-DeWitt, 1983). Many of these machines are linked into the telephone system, which enables them to communicate with other computers and with users in remote locations.

Need for Security Awareness

The business sector is attempting to stay "one step ahead" in the data security problem. Today's managers must be acutely aware of possible breaches to their system--no matter how small or how sophisticated. Business students in university and college business and computer science courses are offered very little in terms of data security awareness. Many instructors include a small segment of computer security topics in an introductory data processing course. Another option is to offer a complete course in EDP audit, which usually requires a strong accounting background, thus eliminating some students being enrolled in that particular course. Unfortunately, very little is being offered in colleges and universities today in terms of general awareness to students who are soon to be entering the business environment and will be faced with the recurring problems of data security (see Appendix A for complete listing of Computer Security: A Manager's Guide").

Curricular Considerations

"Programs must be designed to give the student a broad-based background . . . with a high emphasis on . . . new technological equipment found in the business office" (Loston, 1981, p. 8). "It is up to us as educators to change the thinking philosophy of businesses regarding the capabilities of our graduates through an ongoing means of updating our curricula" (Loston, 1981, p. 8).

In order to keep our curricula as current as possible, we must constantly assess whether or not we are meeting the needs of business. "Business training should be as adjustable and flexible as business. It has to be constantly evaluated, improved, and revised. It is not static; it is dynamic" (Crumley, 1948, p. 14).

Purpose of the Study

The purpose of this study was to provide information indicating whether computer center personnel feel college students in Computer Information Systems programs should become more aware of the importance of computer security. This was accomplished by an interpretative analysis of data obtained from questionnaires mailed to DPMA members on the operational or data processing management level.

Need for the Study

To date, the issue of data security has been addressed individually by managers, computer science educators, computer security analysts, and business faculty. There appears to be a pronounced void in linking the individual approaches to data security and a lack of cohesiveness in the parameters of data security.

Educators have long struggled with the issue of whether to ignore the data security issue in order to avoid opening a "Pandora's Box" or whether to face the issue "head-on" in the hope that the students preparing for business and industry will be cognizant of the problem and will be acquainted through college coursework with the basis of approaching and analyzing the situation. Industry and business, after the students' initial exposure in college, then must acquaint their employees with the specifics of data security that are applicable to their particular environment. In the past, the issue has tended to fall into the "gray" area that educators and industry alike have avoided for fear that too <u>little</u> knowledge could be <u>hazardous</u> and too <u>much</u> could be <u>dangerous</u>.

Limitation of the Study

This study was limited to asking industry respondents to assess the Computer Information Systems (CIS) program within the College or School of Business Curricula. Vocational school curricula was not assessed in order to limit the scope of the study. The study was also limited to a survey of Data Processing Management Association (DPMA) members at the operational or data processing management level, randomly chosen from DPMA's national membership listing.

Definition of Terms

In order to clarify the wide variety of definitions used in the data processing area, the following terms are defined as used in this study:

Access Control - The facilities, procedures, and restrictions for establishing access controls to be enforced by the system.

Access Time - "The time interval between the instant of a request for data from memory and the instant the data is retrieved" (Johnson, 1981, p. 46).

Audit - "The operations developed to correlate the evidence in regard to authenticity and validity of the data that are introduced into the data-processing problem or system" (Sippl and Sippl, 1972, p. 36).

Back up - "Duplicate disk of important data and programs stored as insurance against the possible loss or destruction of an original disk copy" (Johnson, 1981, p. 46).

Communications System -

> A computer system which handles on line, real-time applications . . . . An important element of any communications system are the modems (MODulator/DEModulator) which connect

> the communications multiplexor from the remote output to the interface device in the computer center. On the transmission end, the modulator converts the signals or pulses to the right codes and readies them for transmission over a communication line. On the receiving end, a demodulator reconverts the signals for communication to the computer via the computer interface devise (Sippl and Sippl, 1972, p. 93).

Computer Security (or Data Security) - "Protection of data against unauthorized access or disclosure, and against its intentional or unintentional modification or destruction. Security involves control of, access to, and use of information" (Adams, Wagner, and Boyer, 1983, p. 369).

Control -

> The part of a digital computer or processor which determines the execution and interpretation of instructions in proper sequence, including the decoding of each instruction and the application of the proper signals to the arithmetic unit and other registers in accordance with the decoded information (Sippl and Sippl, 1972, p. 110).

Copy-Protection - "Various methods (often cryptic or diabolical) used to prevent the copying of data or programs from one disk to another" (Johnson, 1981, p. 46).

CRT Terminal (Cathode Ray Tube Terminal) - "An I/O device which uses a television-like screen to display data and a typewriter-like keyboard to input data" (Johnson, 1981, p. 46).

Data - A general term used to denote any or all facts, numbers, letters, and symbols that refer to or describe an object, idea, condition, situation, or other factors. It connotes basic elements of information which can be processed or produced by a computer.

Data Base - "The set of data or information on which operations and conclusions can be based. This is the set of data that is internally accessable to the computer and on which the computer performs" (Sippl and Sippl, 1972, p. 126).

Data Security - The state of data (or information) in which it is safe from unauthorized or accidental modification, destruction, or disclosure (see Computer Security).

E. D. P. (electronic data processing) - Data processing performed largely by electronic equipment (related to automatic data processing).

Embezzlement - To appropriate fraudently for one's own use.

Encryption or Encoding -

1. To apply a code, frequently one consisting of binary numbers, to represent individual characters or groups of characters in a message (synonymous to encipher).

2. To substitute letters, numbers, or characters, usually to intentionally hide the meaning of the message except to certain individuals who know the enciphering scheme (Sippl and Sippl, 1972, p. 163).

Fraud - Deceit, trickery, or breach of confidence, used to gain some unfair or dishonest advantage.

Hacker - "A person who prefers to interact with a computer to the exclusion of all other activities" (Johnson, 1981, p. 47).

Hardware - The mechanical, magnetic, electrical and electronic devices or components of a computer (Sippl and Sippl, 1972).

Identification - "A code number or code name that uniquely identifies a record, block, file, or other unit of information" (Sippl and Sippl, 1972, p. 207).

Input - "Information or data transferred or to be transferred from an external storage medium into the internal storage of the computer" (Sippl and Sippl, 1972, p. 213).

Integrated Networks -

> Basically, two or more interconnected computers with advantages for permitting geographical distribution, and thus economy of computer operations. Such a network also permits parallel processing (usually time-sharing), combinations of send-receive communications, multipoint remote entry and output, locally controlled data banks and switching centers, and less requirement for centralized facilities (Sippl and Sippl, 1972, p. 288).

Memory - "Internal component of a computer where data and programs can be stored temporarily" (Johnson, 1981, p. 47).

Microcomputer - "A computer system designed around a microprocessor as its CPU" (Johnson, 1981, p. 47).

Micrographics - "Information gathering, processing, and retrieval using microfilm technologies and optical display techniques" (Thomas, Schubert, and Lee, 1983, p. 277).

Offsite Storage (or external storage) - "Storage facilities divorced from the computer itself but holding information in the form prescribed for the computer, e.g., magnetic tapes, magnetic wire, punched cards, etc." (Sippl and Sippl, 1972, p. 419).

Operating System -

1. An organized collection of techniques and procedures on operating a computer.

2. A part of a software package (program or routine) defined to simplify housekeeping as input/output procedures, sort-merge generators, data-conversion routines, and tests (Sippl and Sippl, 1972, p. 300).

Output - "Computer results, such as answers to mathematical problems, statistical, analytical or accounting figures, production schedules, etc." (Sippl and Sippl, 1972, p. 310).

Program Modification - "The ability of a program to modify itself or to set a switch so that a set of events occurring at one time can affect the action of the program at a later time" (Sippl and Sippl, 1972, p. 346).

RAM (Random-Access Memory) - "Or memory where each location is uniformly accessible and is often used for the storage of a program and the data being processed" (Johnson, 1981, p. 48).

Reprographics - "Facsimile reproduction of graphic material.

Utilization of many different types of duplicating, printing, and photocopying processes to produce copies" (Thomas, Schubert, and Lee, 1983, p. 243).

<u>ROM</u> (Read-Only Memory) -

> Or memory which cannot be altered either by the user or a loss of power. In microcomputers, the ROM usually contains the operating system and the programming language necessary to make a computer functional once the power is turned on (Johnson, 1981, p. 48).

<u>Sabotage</u> - Any underhanded interference with computer operation.

<u>Software</u> -

> The internal programs or routines professionally prepared to simplify programming and computer operations. These routines permit the programmer to use his own language (English) or mathematics (Algebra) in communicating with the computer (Sippl and Sippl, 1972, p. 407).

<u>Telecommunication</u> - "The transmission or reception of signals, writing, sounds, or intelligence of any nature by wire, radio, light beam, or any other electromagnetic means" (Sippl and Sippl, 1972, p. 447).

<u>Terminals</u> - "An input/output device designed to receive data in an environment associated with the job to be performed, and capable of transmitting entries to, and obtaining output from, the system of which it is a part" (Sippl and Sippl, 1972, p. 450).

<u>User</u> - "Describes a simple person or a group of persons, all of whom have equal rights with respect to accessing a particular body of data and who have a common identity to the system" (Ralston and Reilly, 1983, p. 494).

<u>Vendor</u> - A person or agency that sells products or service.

<u>Word Processing</u> - "The process of creating, modifying, deleting, and formatting textual material" (Johnson, 1981, p. 49).

CHAPTER II

REVIEW OF RELATED LITERATURE

This study was designed to address the issue of computer security by analyzing the opinions of Data Processing Management Association members concerning inclusion of security-related topics into the Computer Information Systems (CIS) curriculum. In order to assess these opinions fully, a thorough review of related literature was conducted to fully address the two main emphasis areas:

1. Review of computer security
2. Curricular concerns relating to computer security

The review of related literature is divided into the following sections in order to cover all parameters of computer security:

1. Losses from Computer Fraud
2. Classification of Breaches
3. Business Installations
4. Data Security Risk Analysis
5. Federal Government Installations
6. World-Wide Security Problems
7. Need for Security Problems
8. Curricular Concerns of Computer Security
9. The ACM Model Curriculum
10. The DPMA Model Curriculum
11. Comparison of ACM vs. DPMA Models

12. Conclusion

The following table is provided to illustrate ~~the extent~~ of the computer security issue: Data Security Risk Analysis Matrix

A complete listing of the ACM and DPMA Model Curricula are provided in Appendices B and C for reference.

Losses From Computer Fraud

Estimates of losses from computer security violations have reached staggering figures in the last few years. Enger and Howerton (1980) address the extent of computer crime as follows:

> The expectations of annual losses from computer fraud range from an estimate of $100 million by the U. S. Chamber of Commerce to an estimate of $3 billion in a recent article published by the Harvard Business Review. According to the U. S. Department of Commerce, only one of 100 such crimes is detected so these figures are only gross estimates. It is further estimated that only 20 percent of computer crimes are reported and even fewer are prosecuted (p. 13).

Potter (1984) states:

> There are no accurate estimates of the total losses to business and to the government each year through computer crimes . . . Many companies and agencies are reluctant to admit that their computer systems are vulnerable to thievery . . . Experts feel that only about one computer theft in 10 is discovered (p. 448).

Classification of Breaches

There are three general types of security breaches:

1. People inside the organization who have enough technical knowledge of the system to enter false commands or to change programs, usually to steal money or materials.

2. People outside the organization who learn enough about the system to break the security codes and enter false commands, usually to steal money.

3. People outside the organization, such as business competitors, who breach the system's security codes to

> obtain information they can use to their own advantage (Potter, 1984, p. 449).

Business Installations

Every computer installation is vulnerable to criminal activity. In the computer environment today, the possibilities of fraud, abuse, and theft are limited only by the criminal's imagination.

> White collar thieves have misused computers to embezzle funds, pilfer time sharing services and programs, eavesdrop on the bids of business competitors, divert inventory, disclose tax and banking records, snatch valuable mailing lists, monitor private medical and pharmaceutical records, print payroll checks and other documents that can be converted into ready cash, reduce and eliminate premiums on insurance and other installment-type payments, and alter transcripts at colleges and universities (Howe, 1982, p. 120).

Too often MIS (Management Information Systems) managers concentrate on hardware and software rather than on personnel as a means of checking computer abuse. "But security is, first and last, a people problem," says Parker (1981, p. 5), Senior Management Systems Consultant at SRI International, a research and consulting firm in Menlo Park, California. The computer environment, from an overall point of view, is defined by:

> . . . corporate policies, operative procedures, and daily practice. From a practical point of view, the security environment has been characterized by and combined with the concept of controls (Hodge, Fleck, and Honess, 1984, p. 414).

Computer crime does not always involve just the loss of money. Loss of vital data--sometimes forever--or such things as invasion of corporate or personal privacy can occur. "Although embezzlement of funds is believed to be the most common form of computer crime" ("Computer Crime," 1981, p. 105) there are other ways in which organizations can suffer such as:

1. Theft of services--employees using computer time for other than company business.

2. Selling or changing information stored in the employer's computer.

3. Invasion of privacy where the victims might sue the negligent organization.

Potter (1984) states:

> There are three general ways to gain unauthorized access to a computer system:
>
> 1. Accidental access
>
>   a. Someone, in normal use of a terminal, accidentally transmits a security code that causes another person's data to be sent.
>
>   b. Often, the person who has done this does not realize what he has done or does not desire to get into someone else's data.
>
> 2. Actively breaking in
>
>   a. Impersonation of an authorized user.
>
>   b. Entry by people who understand the security safeguards and know how to get around them.
>
> 3. Passively breaking in
>
>   a. Wire-tapping a telephone line between a terminal and the computer.
>
>   b. Unauthorized examination of a printout.
>
>   c. The use of microwave receivers to intercept data transmissions from satellites or from long distance telephone relay transmitters (p. 352).

The actual abuses of computers and the potential for even more occurrences are well documented, and research indicates repeatedly that businesses must be aware of the security issue and ward off possible violations <u>before</u> these intrusions occur.

> There is a growing recognition by top management of the need to design computer systems with security as a primary objective and to implement security countermeasures to effectively prevent or deter the exploitation of threats and vulnerabilities . . . (Srinwsasan and Dascher, 1981, p. 1167).

In the May, 1981, issue of Infosystems, Srinwsasan and Dasher suggest that organizational management should formally recognize the need for a computer security program thus ensuring the implementation of effective countermeasures.

In the September 26, 1983, issue of Business Week, the authors suggest that, "above all, management must start taking the break-in problem seriously." Many experts put the blame for poor computer security squarely on top management. To executives at most companies "security is one of the lower priorities" ("Computer Security: What Can Be Done," 1983, p. 127), due mainly to cost justification and concentration on the bottom-line profit. This article goes on to indicate many instances where organizations feel it is difficult to justify investments in security measures.

In addition to guarding the central main-frame computers, the problem is now compounded as organizations must start paying attention to the small personal computers spreading throughout their organizations.

Data Security Risk Analysis

Knapp (1983, p. 23) suggests that "an effective mechanism for convincing management of the importance of data security is the use of the data security risk analysis." Knapp states that "one of the most critical and difficult roadblocks information processing managers face when implementing a data security program is selling the concept to upper-level management" (p. 23). Knapp's Data Security Risk Analysis Matrix includes:

1. Organizational and administrative controls designed to provide effective segregation of duties and restrictions on accessing data, supplemented by the tests of the effectiveness of security protection procedures.

2. Authentication of system users supplemented by the additional verification procedures designed to validate users.

3. Physical security measures designed to provide for continuity of data processing services in the event of natural and man-made disasters, and to control access to computer equipment.

4. Communication line protocol provisions specifically incorporated to provide for data security.

> These controls are labeled as general controls because they apply to all application systems processed within a computer installation.
>
> The data security risk analysis should be organized to evaluate the effectiveness of the general controls within the organization, and to analyze the related risks associated with four general types of security penetration or breach [see Table I] (Knapp, 1983, p. 24).

Hodge, Flech, and Honess (1984) suggest the list of controls should include the following:

1. Internal controls
2. Administrative and physical controls
3. Qualifications and training of staff
4. Data integrity
5. Software integrity
6. Communication controls
7. Cost processing controls
8. Interactive controls.

Federal Government Installations

In a rather lengthy document issued by the Congress of the United States, Office of Technology Assessment, in Washington, D.C., in 1981, entitled Computer Based National Information Systems . . . Technology and Public Policy Issues, the following was excerpted.

The security of computer systems, particularly those operated by

TABLE I

DATA SECURITY RISK ANALYSIS MATRIX

Data Security Controls	Risk Category: Introduction of Unauthorized Data	Unauthorized Program Modification	Unauthorized Disclosure of Data	Inability to Process Data
I. Organizational Structure (Management of Data Security)				
1. Organization's personnel hiring, transferring, termination policies	X	X	X	
2. Organizational responsibility and authority for data security	X		X	
3. Segregation of duties within data processing department	X	X	X	X
II. Authentication/Authorization (Control of remote terminals)				
1. Security facilities of data security sub-system	X	X	X	
2. Password structure, distribution and protection procedures	X	X	X	
III. Activity Logging (Control of program/data files)				
1. Log and review of system assess/usage	X	X	X	
2. Program library protection and maintenance logs		X	X	
3. Access to system programs	X	X	X	
IV. File Integrity Procedures				
1. Data integrity risks	X			
2. Integrity risk related to reconciliation of controls	X			
3. Job control risks	X			
V. Physical Security				
1. Preventive measures against natural and man-made catastrophe				X
2. Unauthorized access	X	X	X	X
3. Back-up/contingency arrangements				X
VI. Controls Over Data Transmission				
1. Communication line protocol provisions for data security	X	-	X	X
Risk Assessment Score	A_i	A_i	A_i	A_i

X = Indicates a Risk Assessment Score should be entered in the matrix

A_i = Total Data Security Risk Assessment

Source: Knapp, 1983.

the Federal Government, has increasingly concerned Congress. Hearings have been held, studies have been published by the general accounting office, and legislation has been introduced, all addressing the problem of meeting threats to federal data installations.

Gibbons (1981) states that:

> It appears that, in general, the Federal Government is rapidly falling behind the private sector in its use and management of up-to-date computer and information technology. The 96th Congress enacted Public Law 96-511 (Paperwork Reduction Act of 1980) to help address this problem. And other issues may arise with respect to the effects of large-scale information systems on Federal decision making (the "automated bureaucracy") and the process by which social values are reflected in information system design (p. 8).

Security concerns have also appeared in congressional reaction to proposals for new advanced information systems by federal agencies, such as the proposed Social Security System, the Tax Accounting System of the Internal Revenue Service, and the upgrading of the National Crime Information Center (NCIC) system of the Federal Bureau of Investigation. All of these proposals have been scrutinized carefully by congressional committees, with particular emphasis on the security of the systems.

Similar concerns have also been expressed by the Executive branch. Presidential Directive 24, published in February, 1979, established policy for the security of federal communications and assigned responsibility for the protection of nonmilitary but sensitive government communications. This directive was motivated by a concern for national security, that is, the potential value of intercepted communications to an enemy (Ruthberg, 1977).

To further set standards on computer security for the federal government, the National Bureau of Standards, Washington, D.C., Institute for Computer Sciences and Technology, approaches the issue of computer security by indicating that computer security is a very complex subject that must be considered from a total system perspective. It involves all the controls necessary to ensure:

(1) the accuracy and reliability of the data maintained on or generated by an automated data processing system,

(2) an appropriate degree of protection of the organizational assets to include the hardware, software, and data from all significant anticipated threats or hazards, and

(3) the economy and efficiency of computer operations.

Computer security, according to the National Bureau of Standards, does not include:

(1) the justification of a computer system

(2) the full range of meeting all management objectives, and determining an acceptable level of risk for an organization, but all are areas for audit involvement (Ruthberg, 1977).

Federal and State Laws Relating to Computer Security

Parker (1981) states that the following Federal and state laws directly relate to computer abuse and theft:

- The Privacy Act of 1974 (Public Law No. 90-579) imposes controls on the data banks containing personal information in federal agencies and among federal contractors. It also established the Privacy Protection Study Commission that has completed its mission and published a series of reports now being used by Congress as the basis for new legislation in the federal and private sectors (p. 98).

  The Foreign Corrupt Practices Act of 1977, which applies to most corporations, corporate managers, and directors, establishes personal liability for noncompliance and sanctions up to $10,000 in fines and up to five years' imprisonment. It also imposes fines on corporations for noncompliance and permits civil suits from stockholders.

The first key provision requires that a corporation 'make and keep books, records and accounts which, in reasonable detail, accurately and fairly reflect the transactions and dispositions of the assets of the issuer.' Computer security is required to assure the safekeeping of computer-stored data representing these records. In addition, security requires the same kind of information for the prevention and detection of crime and error and recovery capabilities.

The second key provision that a corporation must 'devise and maintain a system of internal accounting controls sufficient to provide reasonable assurances that transactions are properly authorized, transactions are properly recorded, access to assets is properly controlled, and assets and asset records are periodically compared.' To be in compliance, a system of cost-effective internal controls must exist in application systems and computer operating systems. These form a major part of the safeguards needed for computer security. Cost-effectiveness requires periodic risk assessments and an ongoing computer security program to assure the implementation of controls to the degree necessary, as indicated by the risks. The law also implies the need for action by management in establishing adequate funding and staffing of computer security programs (p. 99).

- State Computer Crime Laws -- Florida was the first state to enact a computer crime law based on the original 1978 Ribicoff Computer Crime Bill (S 1766).

Its law covers acts for theft of and damage to computer equipment, supplies, programs, and data. It also covers willful, unauthorized access to computers and denial of services to users. The offenses to programs and data apply whether or not the property is stored inside a computer. It applies to programs and data contained in listings, tapes, discs, cards, and other off-line or on-line media. The law does not require the media of storage to be a material object; consequently, electronic pulses would be considered acceptable representations of programs or data and would be subject to the law. This broad definition will facilitate the finding of theft when a program is taken over a telephone line. Because the word 'unauthorized' is not defined by the law and because access is defined so poorly, the intended prohibition against theft of computer services is not clear (p. 100).

The Colorado computer crime law

. . . is modeled on the Florida law but is narrower in coverage because data and programs must be 'contained in the

> computer' to be the subject of the provisions for damage, alteration, or destruction. Further, it appears that theft or fraud involving property that includes electronically representaed data and 'software' must be accomplished by use of a computer to fall within the proscriptions of the law (p. 100).

- Other Applicable Federal Laws --

  Other applicable federal laws include the Federal Copyright Act, theft, miscellaneous theft and theft-related offenses, abuse of federal channels of communication, national security offenses, trespass and burglary, deceptive practices, property damage, and other miscellaneous provisions such as derivative crimes and conspiracy (p. 101).

World-Wide Security Problems

The United States Government and American industry are not the only institutions closely monitoring the problem of computer security. In a study of computer abuse in Australia, the Caulfield Institute of Technology reported that:

> General management tends to be blissfully ignorant of the capabilities, limitations and risk exposures associated with their EDP systems and consciously or subconsciously seem to strive to stay that way. What they are concerned with is efficiency and operating cost. Hence the EDP manager, whilst he may be aware of the dangers faced by the organization won't always feel like sticking his neck out to try to convince management to spend more on tighter controls and better preventative measures ("Study in Computer Abuse," 1979, p. 16).

Need for Security Awareness

After assessing the numerous occurrences of security breaches, it may be imperative to also assess the role of management in the issue of computer security. Hutt (1973) states that:

> . . .the emergence of computer security as a major problem has been caused by the relative success of the computer. . .The rapid growth and acceptance of computer technology has not been accompanied by a parallel growth in the management of this technology. The management lag, coupled with the fact of

> concentration, gives rise to an exposure that can be detrimental to the very existence of even a large organization (p. 41).

The fact that today's organizations are dependent upon data processing services creates a unique vulnerability for many organizations never before experienced in the business environment. Management must recognize the potential risks and identify the consequences for each type of threat.

Absolute security, while unattainable, should not necessarily be eliminated as an objective of a total EDP security program. Reasonable security can be achieved at a moderate cost to the organization.

> Sound management and leadership are essential to a computer security program. Management concern and effort are needed to plan, guide, motivate and control an effective computer security program. A balanced program, with proper concern for human values, will enhance the overall effectiveness of the data processing function (Hutt, 1973, p. 49).

When considering awareness and training of computer security's importance, Ruthberg (1977) suggests two aspects that should be considered:

> - training for those who implement, maintain, and operate the system, and
>
> - training for those who use the system.
>
> The first group should have a more formal training curriculum coupled with an established career path in ADP security administration. A variety of subjects ranging from technical aspects of design and use of ADP hardware and software to the provisions of the Privacy Act should be taught on a regular basis.
>
> The users of the system should be given training on the consequences of a security violation, etc. These users should be examined periodically to ensure that they are properly trained (p. 82).

In a May, 1982, survey conducted by Cook, Eure, Johnston, and Mattord (1982), a questionnaire was mailed to randomly-selected DPMA chapters within the United States. The primary purpose of this study was to determine what current computer users consider important to the area of computer security. About half of the DPMA chapters in the United States surveyed administered the questionnaire to their members. The result was 712 returned questionnaires.

A breakdown of the respondents of the results of the study by Cook, Eure, Johnston, and Mattord (1982) are given below:

--Ninety-three percent of the respondents were from the private sector. The rest were from state and local government, Federal government and colleges and universities.

--Fifty-two percent of the respondents were classified "other managers", while 32 percent were "programmer analysts". Less than one percent were security officers.

--The smallest site had only two employees; the largest, 12,000. There was a mix of small, medium, and large-scale organizations.

--The dollar values of EDP equipment at the various sites ranged from $10,000 to $55 million.

The results of the study by Cook et al. (1982) are summarized in the following paragraphs.

--Physical access protection is important to most institutions. Larger companies with more expensive equipment are more concerned about physical access security than small companies.

--Most computer installations are concerned with disaster protection. Again, more expensive installations show a greater concern for disaster protection than do less expensive installations.

--When rating the effectiveness of procedures to prevent unauthorized data access, larger installations overall considered this area of security more important than small installations--although most of the respondents considered it important to limit unauthorized access.

--About 39 percent of the respondents reporting used either software or hardware encryption. Those reporting with equipment under 1 million used both software and hardware encryption. Almost 65 percent of the small sites reporting used software encryption only, compared to about 28 percent of the larger sites. About 59 percent of the larger sites reported the use of both software and hardware encryption compared to about 18 percent of smaller sites.

--Larger installations carried insurance above the range of depreciated value and closer to replacement value, while small companies were more in the depreciated value range.

--More than 40 percent of companies surveyed neither investigated prospective employees nor bonded key employees. The distribution between companies over $1 million and under $1 million was not drastically different.

--Companies with equipment under $1 million placed considerably less importance on software systems control than the companies with more than $1 million.

--Companies with equipment value of less than $1 million placed less importance than the larger installations on defined rules for data security within application systems.

--Most computer operations consider site backup and other contingency planning much more important than previously thought, larger sites placing far more emphasis in this area than smaller sites.

--Both small and large sites considered backup of programs and data very important (6.11 on a Likert Scale of 1-7).

--Sites under $1 million rated their overall site security 3.83; sites over $1 million rated security 4.87 (on a Likert scale of 1-7).

The authors state in their conclusions that:

> . . . good security is everyone's responsibility--from the lowest echelon to highest management . . . . Many professionals believe that the industry's awareness of the security issue is only the beginning. Computer security is and will continue to be a prime target during the next decade before an acceptable level of sophistication is achieved (Cook, Eure, Johnson, and Mattord, 1982, p. 46).

Another survey conducted in November, 1983, by DPMA shows similar results. Weber (1984), Editor of COMP-U-FAX (The Corporate Information Resource Newsletter) states in the article, "Security Advice for Execs" that:

> Sixty-five percent of the DPMA members surveyed indicated that their organizations allocate a portion of the annual budget to data security. In fact, an average of 2.71 percent of the corporate budget is targeted toward data security . . . . But of those information processing managers who indicated a data security budget, only 40 percent said that it would increase in the next fiscal year. DPMA members also said their organizations would lose an average of $142,676.58 per day in the event of a system failure (p. 1).

Taking a positive attitude that security is everyone's business seems to be a vital concern when considering the issue of data security. Weber (1984, p. 2) reported that "when asked to rank the areas of greatest vulnerability within their organization, DPMA members responded saying DP/MIS staff was most vulnerable to a security breach."

Curricular Concerns of Computer Security

In assessing the computer security issue and management's role in the control of the EDP function, the purpose of this research is also to assess the curricular considerations of the computer security issue.

When evaluating curriculum, the following issues should be considered:

1. Scope - the latitude or the breadth of the curriculum
2. Sequence - the order of time in which educational experiences are to be had.
3. Continuity - continuousness with which the same kinds of experiences are had over a period of time
4. Balance - providing varied but appropriate amounts of experience for learners (Doll, 1970, p. 69).

The two model curriculums reviewed for this study were: ACM Curriculum for Computer Information Systems Education (Association of Computer Machinery) and DPMA Model Curriculum for Computer Information Systems Education (Data Processing Management Association) (see Appendices B and C for complete curriculum content).

The ACM Model Curriculum

> The recommendations of the 1972 and 1973 ACM Curriculum Committee on Information Systems Programs have been influential in the development of degree programs at the bachelor's, master's, and doctoral levels. . . . The report discusses the continuing need for education related to the definition, analysis, design, construction and management of information systems in organizations (Nunamaker, Coufer, and Davis, 1982, p. 781).

Historically, "the ACM Curriculum efforts for information systems (as contrasted with computer science) began with the ACM Curriculum Committee on Computer Education for Management" (Nunamaker, Coufer, and Davis, 1982, p. 781).

ACM goals for an IS (Information Systems) Curriculum are:

1. The IS Curriculum teaches information systems concepts and processes with two contexts, organization functions and management knowledge and technical information systems knowledge, whereas computer science tends to be taught within an environment of mathematics, algorithms, and engineering technology.

2. The IS graduate is expected to work within the environment of an organization and to interact with both organizational functions and computer technology.

3. In technical expertise, the IS curriculum places substantial emphasis on the ability to develop an information system structure for an organization and to design and implement applications.

The graduate of the professional IS program should be equipped to function in an entry level position and should also have a basis for continued career growth. The IS graduate should, furthermore, possess the ability to identify in an ongoing organizational situtation the key issues and problems in each functional area (Nunamaker, Coufer, and Davis, 1982, p. 781).

Even though computer security issues touch every level of the organization, the ACM model curriculum addresses the issue of security specifically only at the graduate level in a subsequent course entitled, Information Systems Policy.

The following is a suggested outline for the course topics:

TOPICS

1. Planning an Organizational Information System (30%)

Information to meet organizational functions, operations, and processes: The information system plan in relationship to organizational strategy and organizational. Effect of organizational learning and stage of development. Selection of projects and establishing of development priorities in the plan. Strategies for achieving information system goals.

Suggested deliveries by student: comprehensive case analysis and high-level master plan defining the application portfolio and classes of data needed by an organizational and priorities for change from existing information system. Also report of the effect on organization of new system and change presentation costs and difficulties.

2. Organizing the Information System Function (20%)

Alternatives for design and placement of information system organization as part of overall organization: centralization, decentralization, division of functions between users and information systems department. Matching information system organization to host organization. Internal organization of information systems department: job functions, flow of work, alternative organizations. Interaction of information system job function with other organizational functions.

Suggested deliveries by students: analysis of case on organization considering restructuring of information systems within organization and case on information system organization considering internal restructuring.

3. Computer Center Administration (10%)

Physical security and backup. Scheduling and control of operations. Quality assurance and error handling. Performance evaluation of operations. Evaluation of alternatives for computer resources: on-site computer, remote job entry, time sharing. Conversion management. Hardware and software acquisition.

4. Management of Information Systems Development (10%)

Strategies and procedures for management of development and maintenance. Project management. Controls and standards. Estimating and scheduling. Implementation management. Evaluation of development.

5. Selection and Development of Information Systems Personnel (10%)

Motivational characteristics of information system personnel selection procedures. Career path planning. Training. Behavioral issues. Strategies for achieving job productivity and job satisfaction. Evaluation.

6. The Social and Legal Environment (10%)

Data privacy. Information access policy. Data security. Contracts.

7. The Information Systems Executive (10%)

A review of the role the information systems manager plays in the organization and a general discussion of the challenges and opportunities associated with the position. Managing the relationship between organizational functions and information systems.

The DPMA Model Curriculum

The primary objective of the DPMA Model Curriculum or Computer Information Systems is:

> To provide graduates with the knowledge, abilities, and attitudes to function effectively as application programmer/analysts, and with the educational background and desire for lifelong professional development (Athey, 1981, p. 10).

The specific curriculum objectives of the DPMA Curriculum are:

1. To provide understanding of the goals, functions, and operations of business organizations;

2. To provide understanding of the information needs and the role of information systems in these organizations;

3. To provide the analytical and technical skills for identifying, studying, and solving information problems within organizations;

4. To provide communications and human relations skills for effective interaction with organization members, especially with the users and developers of information systems;

5. To provide knowledge and ability for effective management of information systems projects;

6. To instill a professional attitude and seriousness of purpose about Computer Information Systems as a career field; and

7. To provide the background for further study of and professional advancement in the field of Computer Information Systems (Adams and Athey, 1981, p. 10).

The Computer Information Systems (CIS) Model Curriculum contains three main elements, according to Pierson (1984):

1. Seven required CIS core courses
2. Three additional CIS courses to be chosen from eight selective offerings
3. A minimum set of business support courses.

Since the DPMA Model Curriculum was first published in 1982, more than 4,000 copies have been distributed to educators, educational administrators, and information systems professionals.

> As part of this ongoing project to support Computer Information Systems (CIS) education, DPMA has standing committees that carry on the continuing development and refinement of curriculum recommendations and track the progress of colleges and universities implementing them . . . . Understanding the current status of CIS education is a necessary prerequisite to designing mechanisms that promote future growth and development (Souder and Adams, 1984, p. 40).

In contrast to the ACM curriculum, the DPMA Model Curriculum suggests several courses where EDP security concepts may be introduced.

CIS-1 Introduction to Computer-Based Systems

<u>Topic: Future of Computers in Society (10%)</u>

> Trends in hardware and software technology. Trends in distributed data processing, database management systems, and administration. Networks, switching, and protocols, and office of the future. Merging of data processing, word processing and communications. Concepts of packaged software, firmware, and natural languages. Standardization in the

industry. Effects of computers in organizations and individuals. Computer errors. Implications of data banks for personal and commercial privacy. Computer crime, vulnerability and security. Forms of physical and logical safeguards. Administrative controls and EDP auditing. Data processing legislation. Computer selection and contracts. Employment opportunities, including applications programmer, maintenance programmer, systems programmer, systems analyst, data base administrator, project leader, operations manager, data processing manager. Career tracks from data entry to overall management of data processing and information systems. Certification for computer professionals (Adams and Athey, 1981, p. 23).

CIS-13 Audit and Controls

1. EDP Audit Environment and Computer Information Systems (10%)

The EDP audit environment and its relationship with and effect on computer-based information systems. Relationships between the internal audit function, the external audit function, the public accounting function and the information systems function. EDP audit definitions. Discussion of major examples of computer abuse and their impacts on the business community.

2. Information Systems Controls (25%)

Types of information systems controls: application controls, system development controls, information processing facility controls and horizontal control versus vertical controls. Preventive, detective and corrective controls. Controls and security.

3. Computer Audit Techniques (30%)

Types of EDP audits: audits of applications, audits of systems development, audits of information processing facilities and SAS-3 reviews. Computer-assisted audit techniques such as test decking, integrated test facility, parallel simulation, system control audit review file, sample audit review file, snapshot, extended records, etc.

Uses of audit software to verify results: confirmation, comparison with file or physical and edit and reasonableness tests. Advantages and disadvantages of computer-assisted audit techniques.

4. Auditing Advanced Information Systems (20%)

Techniques used to audit advanced systems which utilize a combination of any one of the following information processing techniques: on-line, real-time, teleprocessing, telecommunication, distributed processing, minicomputer, microcomputer, data bases, etc. Techniques used to audit data base systems. Cost of advanced controls. Audit technical expertise needed. Examination of minicomputer and microcomputer applications and environment.

5. Systems Approach to Auditing (15%)

Concept and application of risk assessment. Concept and application of threat analysis. Concept and application of cost/benefit analysis in analyzing exposures and recommending controls (Adams and Athey, 1981).

Comparison of ACM vs. DPMA Models

Vanacek and Guynes (1981-82, p. 18) in comparing the two curriculums state: "Both curriculum development activities seem to have zipped along as though the other did not exist." The authors state that "both curriculums attempt to cover about the same topics when viewed superficially." Their conclusion is that "the DPMA curriculum has done a much better job of maintaining the business emphasis within their curriculum while the ACM curriculum still has the computer science orientation."

Conclusion

In relation to the issue of computer security, it would appear that the DPMA model does, in fact, suggest more than a superficial view of the security problem, particulary in the EDP audit course.

The purpose of this study is to assess whether or not more emphasis should be given (1) throughout the curriculum or (2) as a separate course, to the issue of data security in order to update the curriculum with today's current issues. The input by industry is vital in terms of curriculum asssment in order to avoid the "trendiness" of adding topics and courses that may not transcend and be relevant in the future.

Knapp (1983, p. 23) suggests that "a data security 'frame of mind' and discipline must be developed." Mr. Bill Stanley of Conoco, Inc., Ponca City, Oklahoma, added this relevant comment to his response to the research pilot questionnaire that was mailed to him for this study: "It is more important to teach data security as an <u>attitude</u> rather than as a <u>technology</u>. Most businesses have common attitudes toward data security but the technology can vary between companies and vendors."

The teaching of <u>attitude</u> might well guide educators when considering curricular changes in the computer environment. Technology will indeed change and update but an ethical, moral attitude toward computer security <u>must</u> remain constant.

CHAPTER III

DESIGN AND PROCEDURES

This study was designed to obtain data from selected members of the Data Processing Management Association (DPMA) concerning their opinions concerning inclusion of computer security topics into the Computer Information Systems (CIS) Program in collegiate schools of business. For the purpose of clarification, computer security may be defined as any activity that involves the functions of avoidance, deterrance, prevention, detection, recovery, and correction of data so that privacy and security of the data and equipment are not violated.

Detailed descriptions of the procedural steps in the study included in this chapter are as follows:

1. Sample Selection
2. Development of the Study Instrument and Cover Letter
3. Pretesting the Study Instrument (Pilot Study)
4. Mailing of the Study Instrument
5. Follow-up Letter and Mailing
6. Statistical Analysis of the Questionnaire Responses
7. Summary

The principal objectives of this study are:

1. To determine if data processing managers believe there is a need for students enrolled in the CIS program in colleges and universities to develop some basic knowledge of computer security while pursuing their college degrees.

2. If respondents answer "no" to the apparent need question, there will be an attempt to determine why these data processing managers see no apparent need at this point in the education process to include computer security topics.
3. If the data processing managers believe there is a need to acquaint students with the basic elements of data security (indicated by a "yes" response), the following information will be obtained:
    a. The recommendation that data security be offered as a complete course in the curriculum. A listing of potential topics will be listed and respondents will be asked to indicate the topics they believe would be relevant.
    b. If the respondents believe that data security should be incorporated into various courses throughout the curriculum, the respondent will be asked to check off courses from the Data Processing Management Association's (DPMA) Model Curriculum that may possibly be considered for inclusion.

By analyzing the results given by the respondents, the researcher will be able to obtain current information from data processing managers concerning:

1. Whether a college or school of business should be offering a separate course in data security;
2. Whether data security should be offered as an incorporation into courses throughout the Computer Information System (CIS) curriculum;
3. Whether the topic of data security should not be offered in any form in the curriculum.

Sample Selection

The respondents selected for this study are members of the Data Processing Management Association (DPMA). After considering several other groups for the study, it was decided that DPMA members should be queried as they represent a broader grouping of data processing professionals than other groups. DPMA is one of the largest world-wide organizations serving the information processing and computer management community. It is comprised of all levels of management personnel and, through its educational and publication activity, DPMA seeks to encourage high standards of performance in the field of data processing and to promote a professional attitude among its members.

DPMA's support of research and inquiry is stated in its international bylaws as follows: "To foster, promote and develop education and scientific inquiry in the field of data processing and data processing management" (Ralston and Reilly, 1984, p. 492).

The sample of 700 DPMA members chosen to be surveyed were in the Data Processing and Operational Management category (Job Function Category B). These 700 members were randomly selected from the United States listing only. Foreign countries were excluded in order to limit the scope of the study.

The mailing list was purchased from:

Data Processing Management Association
International Headquarters
505 Busse Highway
Park Ridge, Illinois 60068-3191

The 700 members were selected at random by DPMA from the approximately 16,000 members in category B prior to their printing the listing. (See Appendix F for correspondence relating to the mailing list.)

Development of the Study Instrument and Cover Letter

The study instrument designed to gather data for this study was a six-page questionnaire. After thoroughly reviewing literature relating to questionnaire design, analysis of numerous sample questionnaires, and consultations with various faculty members in both the College of Business and Department of Applied Behavioral Sciences at Oklahoma Stae University, the completed questionnaire was printed on both sides of 8-1/2 x 11 sheets to facilitate ease of completion by the potential respondent.

The questionnaire was designed according to guidelines stated by Bowman and Branchaw (1984) and could be completed in approximately 15 minutes by the respondent.

The six sections of the questionnaire were:

I. Business Information

- Includes computer equipment at respondent's location, number of employees, whether designated person is responsible for computer security, title of person directly responsible for computer security.

II. Personal Information

- Includes position of respondent, years in respondent's present position, how long respondent has been employed in a computer-related position, highest educational level of respondent, education or training of respondent in computer security, how many emploees respondent supervises, membership in data processing professional organization, familiarity with various Computer Information Systems Model Curricula.

III. <u>Need for Computer Security Knowledge</u>

- Includes whether respondent feels computer center employees should possess some knowledge about computer security. If "no", gives the respondent choices on reasons for "no" response. The "no" respondent then goes to Section V. If "yes", the respondent goes on to Section IV.

IV. <u>Analysis of Computer Security Topics</u>

- Respondent indicates the importance of various topic areas that might be considered for inclusion in the Computer Information Systems (CIS) Curriculum relating to the topic of computer security. A rating scale of 1-5 is used with 1 representing Very Important and 5 representing Very Unimportant.
- Respondent is asked to indicate the method to <u>best</u> develop computer security knowledge. The choices are:
    A. Complete course in computer security in addition to incorporation of computer security topics in the Computer Information Systems Curriculum.
    B. Complete course in computer security ONLY.
    C. Incorporation of computer security topics into the current courses in the Computer Information Systems (CIS) Curriculum ONLY.
- Using the <u>DPMA Model Curriculum for Undergraduate Computer Information Systems Education</u>, the respondent is asked to rate the importance of inclusion of computer security topics into the DPMA Model Curriculum, using a scale of 1-5, where 1 represents Very Important and 5 represents Very Unimportant. (See Appendix B for DPMA Model Curriculum.)

V. Optional

- Respondent may include name, organization, address, and position. Also includes instructions for returning the completed questionnaire.

VI. Additional Comments

- provides space for additional comments and suggestions relating to the questionnaire, the study being conducted, or the subject of computer security.

An identification number was written in the top right-hand corner to be used for follow-up purposes on the second mailing. (See Appendix E for the study instrument.)

The cover letter used appeals to professionalism and cooperation, citing the growth of data security violations in recent years. The main emphasis was that the respondent's input would greatly aid in the assessment of current college curricula in the CIS area. The cover letter was signed by both the researcher and dissertation chairperson, Dr. Herbert M. Jelley. The cover letter was offset print on Oklahoma State University College of Business Administration letterhead to aid in professional appearance. (See Appendix E for cover letter.)

Pretesting the Study Instrument (Pilot Study)

After careful consideration of the design of the questionnaire and cover letter, a pilot study was mailed on February 13, 1984, to the following in order to pretest the questionnaire and cover letter:

1. Researcher's doctoral committee members.
2. Five information processing instructors in the College of Business Administration at Oklahoma State University.

3. Two statisticians in the Department of Statistics at Oklahoma State University.
4. Two instructors in Educational Research/Statistics in the Applied Behavioral Studies Department at Oklahoma State University.
5. Three employees of the Oklahoma State University Computer Center.
6. One Director of Management Information Systems at Oklahoma State University.
7. One faculty member of Management Information Systems, Department of Management, College of Business Administration, Oklahoma State University.
8. Twelve managers of data processing centers located in Oklahoma, Illinois, and Texas. These names were provided by Mr. Davis Sellers, Instructor in the Information Processing Program, Department of Administrative Services and Business Education, College of Business Administration, Oklahoma State University. Mr. Sellers has been employed for several years in computer-related positions in the Tulsa area and was acquainted with each of the industry persons on the pilot study. These data processing managers were chosen as they closely resembled the targeted population to be receiving the actual questionnaire.

A letter thanking all pilot study respondents for their participation and assistance in revising the questionnaire was sent to both the respondents at Oklahoma State University and respondents in industry. (See Appendix D for thank-you letter.)

Mailing of the Study Instrument

After the appropriate revisions were made according to suggestions given from the pilot study respondents, the questionnaire was mailed to 700 randomly selected DPMA members. Self-sticking labels printed by DPMA were adhered to Oklahoma State University College of Business Administration envelopes with the researcher's name stamped above the return address (see Appendix E for envelopes). A self-addressed Oklahoma State University Central Mailing Services envelope with the researcher's name stamped at the bottom-left corner was included along with the cover letter and study instrument, thus enabling the respondent to return the completed study instrument easily. (See Appendix E for return envelope.)

Funding for the initial and return mailings was provided by a doctoral dissertation funding grant awarded to the researcher by the Office of Business and Economic Research, College of Business Administration, Oklahoma State University.

Envelopes containing the initial mailing were sent on April 6, 1984, and the response date for completion and return was stated as May 1, 1984.

Follow-up Letter and Mailing

Approximately one week after the initial mailing deadline, a follow-up mailing was sent to those DPMA members who did not respond to the initial mailing. The identification numbers on the returned questionnaires were used to identify those responding. Using a duplicate DPMA mailing list, the non-respondents were drawn from the list of those whose labels had not been removed when the initial questionnaire was returned.

Using the same questionnaire as in the first mailing, the nonrespondents were then sent a follow-up letter and a second copy of the questionnaire. The only change that was made to the questionnaire was that the color was changed to green (initial mailing was blue) in order to determine whether the response was from the first or second mailing.

The follow-up mailing was sent on May 7, 1984, and the response date was given as June 1, 1984. (See Appendix E for a copy of the follow-up cover letter.)

The response rate for the mail survey was 43.8 percent calculated by the following method recommended by Dillman (1978):

$$\text{Response Rate} = \frac{\text{Initial Mailing Number Returned}}{\text{Number in Sample} - \text{(noneligible and nonreachable)}} \times 100$$

$$\text{Response Rate} = \frac{\text{299 Returned}}{\text{700 in Sample} - \underset{\text{(ineligible and nonreachable)}}{9 + 9}} \times 100 = 43.8\%$$

A further breakdown of the percentages of returns and nonreturns is shown in Table II on the following page.

Statistical Analysis of the Questionnaire Responses

The responses gathered from the study instrument were coded and transformed into computer readable format utilizing the NCS Trans-optic MBO-15514-321 scanner sheets provided by the Bureau of Tests and Measurements, Oklahoma State University.

The SPSS-X (Statistical Package for the Social Sciences) was used

TABLE II

DISTRIBUTION OF QUESTIONNAIRE RETURNS AND NONRETURNS

Category	Number	Percent
Total Number in Population (First Mailing)	700	100.0
Total Returns from the First Mailing	217	31.0
Total Returns from the Follow-up Mailing	91	13.0
Total Respondents	308	44.0
(Both mailings)	308	44.0
Non-Respondents (Both mailings) (Data incomplete and unuseable)	9	.01
Returned Questionnaire (Respondent unreachable due to outdated address)	9	.01
Response Rate		43.8

to determine frequencies, cross tabulations, descriptive and demographic statistic rankings, and Chi-squares. According to the Oklahoma State Computer Center User Manual (Second Edition, 1984, p. 4134), "SPSS-X is an integrated system of computer programs for the analysis of social science data. The system has been designed to provide the social scientist with a unified and comprehensive package enabling him to perform many different types of data analysis in a simple and convenient manner. SPSS-X is a major revision of SPSS . . . most of the changes between SPSS and SPSS-X affect file definition."

Using the SPSS-X statistical package, the data analysis will be divided in five sections:

Section I - Frequency Distributions

Percentages are calculated on demographic information (both business and personal), analysis of need for computer security knowledge, analysis methods to best develop computer security knowledge. Since many of these questions elicited more than one response, multiple responses are duly noted with the appropriate table.

Section II - Rankings of Topics by Mean

Using means as the criteria for ranking, the topics listed in IV-1 of the questionnaire are ranked on a Likert scale of 1 - 5.

Section III - Rankings of Courses by Mean

Using means as the criteria for ranking, the core and elective courses listed in IV - 3 of the questionnaire are ranked on a Likert scale of 1 - 5.

Section IV - Cross Tabulations

Cross tabulations of III - 1 of the questionnaire, requesting the respondent's opinion concerning the need for computer security knowledge (indicated by a "yes" or "no" response are cross-tabulated with:

1. Number of employees in the computer center
2. Whether organization has a designated security person(s)
3. Title of person directly responsible for computer security
4. Number of employees directly responsible for computer security
5. Respondent's present position
6. Number of years respondent has been in his/her present position
7. Number of years respondent has been employed in a computer-related position
8. Respondent's highest educational level
9. Respondent's major field of study
10. Computer security training untilized by the respondent
11. Number of employees supervised by respondent
12. Respondent's membership in professional organizations
13. Respondent's familiarity with model curricula
14. Best method to develop computer security knowledge

The "yes" responses and the "no" responses were tabulated separately to be able to compare the results of the two responses.

These same criteria (1-14) were then compared to the question in Section IV - 2 of the questionnaire where the respondents were asked their opinions on methods that would <u>best</u> develop computer security knowledge.

Section V - Chi-square

The same criteria used in the cross-tabulations were then analyzed using Chi-squares in order to test for significance.

This chapter described the survey instrument, the survey procedures, and the method of data compilation and analysis.

A thorough analysis of the data interpretation is given in Chapter IV. Conclusions and recommendations made on the basis of these findings are reported in Chapter V.

A detailed description of the development of the study instrument was presented, as well as the pilot study and original and follow-up mailings. The study instrument and cover letter are exhibited in Appendix E.

CHAPTER IV

ANALYSIS OF DATA

The study instrument (questionnaire) was sent to 700 Data Processing Management Association (DPMA) members, randomly selected from category B of the members in the data processing or operations management group, categorized by job function. These DPMA members were selected from all 50 states of the United States and, thus, represented a nationwide sampling.

The data gathered from the study instrument focused on these DPMA members' opinions concerning inclusion of computer security topics into the Computer Information Systems (CIS) program in collegiate schools of business. Data was obtained from the respondents regarding the following:

- The educational background and work histories of the DPMA members.
- Opinions concerning importance of selected computer security topics to be considered for inclusion in the Computer Information Systems (CIS) curriculum.
- Opinions concerning methods to best develop computer security knowledge.
- Opinions concerning importance of inclusion of elements of data security into the various core and elective courses within the CIS.

The findings resulted from a detailed analysis of the responses to the study instrument.

The items selected for inclusion in the study instrument were chosen after thoroughly reviewing literature relating to questionnaire design, analyses of numerous sample questionnaires, and consultations with various faculty members in both the College of Business Administration and the Department of Applied Behavioral Sciences at Oklahoma State University.

As a pilot study, the study instrument was sent to various faculty members and computer center managers in both industry and university operations (Chapter III contains a complete listing of the pilot study members).

Allowances for "other" responses that may not be included in the statement of the question were made throughout the questionnaire in order to include all possible responses.

Plan for Analyzing the Gathered Data

Section I of the study instrument was designed to obtain from the DPMA members selected data regarding business information as follows:

- Computer equipment presently being utilized in the respondent's operation.
- Number of employees presently employed in the respondent's computer center.
- Whether the respondent's computer center has a designated person directly responsible for computer security.
- Number of people in the respondent's organization who are directly responsible for computer security.

- The title of the person(s) directly responsible for computer security.
- Reasons for not having a designated person responsible for computer security.

Section II of the study instrument was designed to obtain data from the selected DPMA members regarding the following personal information:

- Respondent's present position.
- Length of time that the respondent has been employed in his/her present position.
- Length of time that the respondent has been employed in a computer-related position.
- The respondent's highest educational level. A space was also provided for the respondent to specify their major area of study.
- Educational or training areas that the respondent has utilized in computer security.
- Number of employees that the respondent directly supervises at the present time.
- Professional organization(s) in which the respondent currently holds memberships.
- The respondent's familiarity with selected Computer Information Systems (CIS) Model Curricula.

Section III of the study instrument requests the respondent's opinion concerning the need for computer security knowledge by persons employed in computer centers. Respondents indicating a "no" response to need are then requested to choose an appropriate response for their response. The "no" respondents are then requested to exit the study instrument. Those respondents indicating a "yes" for need are then asked to continue with the remainder of the study instrument.

Section IV is completed by only those respondents indicating a "yes" response in Section III, indicating that they feel computer center employees should possess knowledge about computer security. The respondents are asked the following: Rate the importance of 18 topic areas that relate to computer security. A Likert scale was utilized using the following scale:

1 - Very Important

2 - Important

3 - Average Importance

4 - Unimportant

5 - Very Unimportant

- Indicate the methods that would best develop computer security knowledge by choosing from a listing of options.
- Rate the importance of including elements of computer security into the seven core and eight elective courses listed in the Computer Information Systems (CIS) Curriculum. Course titles and descriptions were taken from the "DPMA Model Curriculum for Undergraduate Computer Information Systems Education" (Adams and Athey, 1981).

The following Likert rating scale was utilized:

1 - Very Important

2 - Important

3 - Average Importance

4 - Unimportant

5 - Very Unimportant

Section V is optional and asks the respondent to fill in his/her name, organization, address, and position.

Section VI provides the respondent space for any additional comments and suggestions he/she may have relating to the questionnaire, the study being conducted, or the subject of computer security.

A Statistical Package for the Social Sciences (SPSS-X) program was utilized to tabulate the responses to each item of the questionnaire. The results of each response were tabulated according to frequency of occurrence, cumulative frequency, percentage, and cumulative percentage. Two-way tables (cross tabulations) were used to compare the respondent's business and personal information with the results in Section IV. Chi-squares were also computed on the cross tabulations.

Tables of specific findings are presented in the following discussion. Interpretation of the statistics follows each table.

Data Analysis

Responses were received from 299 DPMA members throughout the United States. Nine of these responses were deleted from the population for the following reasons:

1. One respondent indicated that his/her installation no longer had a computer.
2. One respondent felt he/she could better analyze the topic of data security by using a narrative format. The comments given will be included in the listing of "Additional Comments" at the end of Chapter IV.
3. One respondent indicated that he/she was employed at a

remote job entry site and the mainframe computer was located in another state. The respondent indicated that he/she was, therefore, unable to respond to the questionnaire.

4. One respondent failed to complete Section III which deals with the need for computer security knowledge and failed to complete various portions of Section IV which deals with the analysis of computer security topics.
5. Five respondents failed to complete various portions of Section IV which deals with the analysis of computer security topics.

Three returned questionnaires were deleted as the respondent returned both the original and the follow-up questionnaire. In all three cases, the original response was used and the follow-up response was deleted so that only one response per DPMA member was added to the total data analysis.

A total of nine questionnaires were returned to the researcher with indications from the United States Postal Service of:

- Insufficient address
- Moved--left no address
- Moved--not forwarded
- Address unknown
- Forwarding order expired
- Unclaimed
- Return to sender

There were 290 questionnaires returned that were used for the analysis of the data. The analysis is divided into seven sections:

1. Frequency distributions that analyze the use of electronic data processing by the respondent's firm, an analysis of the personal information about the respondent, and analysis of the business information about the respondent.
2. Ranking by means of computer security topics.
3. Ranking by means of courses, both core and elective, from the DPMA Model Curriculum.
4. Cross tabulations of Sections 2 and 3 above where comparisons are made between demographic data (Sections I and II of questionnaire) and selected security topics and core and elective courses.
5. Chi-squares on Section IV to test for significance.
6. An Interpretative Summary of the respondents' narrative comments.
7. Summary.

Section I - Frequencies

The first portion of the study instrument, regarding the analysis of the use of electronic data processing by the respondent's firm, was subdivided into six areas:

1. Make and model of computer presently being utilized for the respondent's operation.
2. Number of people presently employed in respondent's computer center.
3. Whether respondent's computer center has a designated person(s) directly responsible for computer security.
4. Number of people in respondent's organization directly

responsible for computer security as stated in the job description.

5. Title of person(s) directly responsible for computer security.
6. If respondent checked "no" in number three indicating that there was no designated person directly responsible for computer security, this position analyzes the reasons for the "no" response. Each of the six areas was analyzed using frequencies and percentages.

Make and Model of Computer (Section I-1 of Questionnaire)

Since the respondent could check all that applied, many respondents had multiple responses to this item. A total of 431 responses were given by the 290 respondents.

IBM, as was anticipated, tended to dominate the utilization with 198 respondents, or 45.9 percent, indicating that their computer operation utilized that particular make. Apple was utilized by 29 respondents, or 6.7 percent. Hewlett Packard was used by 26 respondents, or 6.0 percent. Burroughs was used by 25 respondents, or 5.8 percent. Radio Shack was used by 14 respondents, or 3.3 percent. NCR (National Cash Register) was used by 10 respondents, or 2.3 percent (see Table III).

A total of 129 respondents, or 30.0 percent, indicated that they used computer makes other than those listed on the questionnaire. These computers are listed in Table IV.

TABLE III

MAKE OF COMPUTER PRESENTLY UTILIZED BY RESPONDENT'S COMPUTER CENTER OPERATION

Make	Frequency	Percent	Valid Percent	Cumulative Percent
IBM	198	45.9	45.9	45.9
Burroughs	25	5.8	5.8	51.7
Hewlett Packard	26	6.0	6.0	57.7
NCR	10	2.3	2.3	60.0
Apple	29	6.7	6.7	66.7
Radio Shack	14	3.3	3.3	70.0
Other	129	30.0	30.0	100.0
Total	431**	100.0	100.0	

*Other-hand tallied.

**Multiple responses.

TABLE IV

OTHER MAKES OF COMPUTER EQUIPMENT UTILIZED BY RESPONDENT'S COMPUTER CENTER OPERATION

Make	Number of Respondents
Four Phase	1
Tektronix	2
Texas Instrument	8
Data General	2
Amdahl	5
Honeywell	11
Digital Equipment	38
ACTOS	2
ONYX	2
Control Data	2
Sperry Systems	7
Epson	2
WANG	4
Univac	2
Microdata	3
QANTEL	4
COMPAQ	2
SANYO	2
Data General	5
NS 1000	1
Xerox	2
SDS	1
Perkin-Elmer	3
North Star Horizon	2
Data Point	4
U. S. Design Corporation	2
Mohawk	2
Superbrix	1
Intertec-CAD	1
Harris	2
ITEL	1
NAS	3
Total	129

Due to the number of responses involved, the "other" responses are not broken down by percentages in Table IV. A breakdown of model numbers used by the respondents for the six categories listed on the questionnaire are shown in Table V.

Number of People Presently Employed in Respondent's Computer Center (Section I-2 of Questionnaire)

Table VI indicates that 171 respondents,or 59.0 percent had from 1 - 20 employees in their computer center. Forty respondents, or 13.8 percent, indicated that there were from 21 - 40 employees. Twenty-four percent indicated that their computer center had from 41 - 60 people. Seven, or 2.4 percent, indicated that their computer center had from 61 - 80 employees. Thirteen percent indicated that their computer center employed from 81 - 100 persons. Thirty-five, or 12.1 percent, of the respondents had over 100 employees in their computer center.

Of the 35 respondents who indicated that the number of people presently employed in his/her computer center was over 100, the breakdown is listed in Table VII.

Number of Computer Centers Having a Designated Person Directly Responsible for Computer Security (Section I-3 of Questionnaire)

The "yes" and "no" responses were not spread very widely. There were 141 "yes" responses (48.6 percent) indicating that their computer center had a designated person directly responsible for computer security. The "no" responses were slightly greater in number with 149

TABLE V

MODEL OF COMPUTER UTILIZED BY RESPONDENT'S COMPUTER CENTER OPERATION

Value	Frequency	Percent	Valid Percent	Cumulative Percent
<u>IBM</u>				
4341 (includes PC)	63	31.8	31.8	31.8
3083	22	11.1	11.1	42.9
4331	8	4.0	4.0	46.9
3033	19	9.7	9.7	56.6
3031	3	1.5	1.5	58.1
370	8	4.0	4.0	62.1
System 34	14	7.1	7.1	69.2
System 36	3	1.5	1.5	70.7
System 38	14	7.1	7.1	77.8
Series I	4	2.0	2.0	79.8
4361	8	4.0	4.0	83.8
3081	11	5.7	5.7	89.5
System 3	3	1.5	1.5	91.0
5340	3	1.5	1.5	92.5
5120	4	2.0	2.0	94.5
4381	2	1.0	1.0	95.5
8100	2	1.0	1.0	96.5
4300	3	1.5	1.5	98.0
3651	1	.5	.5	98.5
2031	1	.5	.5	99.0
3084	2	1.0	1.0	100.0
Total	198	100.0	100.0	
<u>Burroughs</u>				
B 800	2	8.0	8.0	8.0
B 2900	2	8.0	8.0	16.0
B 1955	8	32.0	32.0	48.0
B 1905	3	12.0	12.0	60.0
B 1985/1855	4	16.0	16.0	76.0
B-92	3	12.0	12.0	88.0
B-1990	3	12.0	12.0	100.0
Total	25	100.0	100.0	

TABLE V (Continued)

Value	Frequency	Percent	Valid Percent	Cumulative Percent
Hewlett Packard				
3000 Series	11	42.3	42.3	42.3
1000 Series	4	15.4	15.4	57.7
HP-100	2	7.7	7.7	65.4
Model 44	2	7.7	7.7	73.1
Model 48	3	11.5	11.5	84.6
HP-800	4	15.4	15.4	100.0
Total	26	100.0	100.0	
NCR				
8450	1	10.0	10.0	10.0
8565	1	10.0	10.0	20.0
NAS-5	1	10.0	10.0	30.0
8251	4	40.0	40.0	70.0
DPI	1	10.0	10.0	80.0
725	1	10.0	10.0	90.0
8271	1	10.0	10.0	100.0
Total	10	100.0	100.0	
Apple				
II^{e}	12	41.4	41.4	41.4
III	2	6.9	6.9	48.3
Lisa	4	13.8	13.8	62.1
II	8	27.6	27.6	89.7
MacIntosh	3	10.3	10.3	100.0
Total	29	100.0	100.0	
Radio Shack				
Model 1	4	28.6	28.6	28.6
TRS-80 Series	10	71.4	71.4	100.0
Total	14	100.0	100.0	

TABLE VI

NUMBER OF PEOPLE PRESENTLY EMPLOYED
IN RESPONDENT'S COMPUTER CENTER

Number of People	Frequency	Percent	Valid Percent	Cumulative Percent
1 - 20	171	59.0	59.0	59.0
21 - 40	40	13.8	13.8	72.8
41 - 60	24	8.3	8.3	81.0
61 - 80	7	2.4	2.4	83.4
81 - 100	13	4.5	4.5	87.9
Over 100	35	12.1	12.1	100.0
Total	290	100.0	100.0	

Table VII

BREAKDOWN OF OVER 100 RESPONSES REGARDING NUMBER OF PEOPLE PRESENTLY EMPLOYED IN RESPONDENT'S COMPUTER CENTER

Number of People		Frequency	Accumulation
101-199	105	1	
	115	1	
	123	1	
	138	1	
	140	3	
	149	1	
	150	2	
	160	1	
	162	1	
	164	1	
	181	1	
	185	1	
	190	1	
Subtotal		16	16
200-299	200	2	
	220	1	
	250	2	
Subtotal		5	21
300-399	320	1	
Subtotal		1	22
400-499	450	1	
Subtotal		1	23

TABLE VII (Continued)

Number of People		Frequency	Accumulation
500-599		0	
Subtotal		0	23
600-699	600	1	
Subtotal		1	24
700-799	___	0	
Subtotal		0	24
800-899	___	0	
Subtotal		0	24
900-999	1	1	
Subtotal		1	25
1000-1099	___	0	
Subtotal		0	25
1100-1199	___	0	
Subtotal		0	25
1200-1299	1200	1	
Subtotal		1	26
	Total of "over 100" who indicated number:		26
	There were nine respondents who checked "over 100" but did not provide a number:		9
Total			35

respondents, or 51.4 percent, indicating that their computer center did not have a designated person.

Number of People in Respondent's Organization Directly Responsible for Computer Security (Section I-4 of Questionnaire)

The 141 respondents who indicated that their computer center had a designated person (Table VIII) were then asked to list the number of persons directly responsible for computer security. The breakdown is shown in Table IX.

The number of persons responsible for security tends to be rather small in number. Sixty-four, or 22.1 percent, indicated that they had one person. Forty eight respondents had two. In the five, six, seven or more categories, the number becomes much smaller with two, one, three listed, respectively (.7, .3, and 1.0 percent).

Title of Persons Directly Responsible for Computer Security (Section I-5 of Questionnaire)

The titles given to persons directly responsible for computer security vary from organization to organization. Table IX details the breakdown of these various titles. The first three titles (Security Analyst, Operations Analyst, and Director of Computer Security) were listed on the questionnaire. The remaining three groupings were hand tallied by the researcher for ease of interpretation.

Fifty-five respondents, or 17.1 percent, had the title Data Processing or Information Systems Director or Manager. One-hundred-thirty, or 40.4

TABLE VIII

NUMBER OF COMPUTER CENTERS HAVING A DESIGNATED PERSON DIRECTLY RESPONSIBLE FOR COMPUTER SECURITY

	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	141	48.6	48.6	48.6
No	149	51.4	51.4	100.0
Total	290	100.0	100.0	

TABLE IX

NUMBER OF PEOPLE IN RESPONDENT'S ORGANIZATION DIRECTLY RESPONSIBLE FOR COMPUTER SECURITY

Value	Frequency	Percent	Valid Percent	Cumulative Percent
0	149	51.4	----	----
1	64	22.1	45.4	45.4
2	48	16.6	34.0	79.4
3	14	4.8	9.9	89.4
4	9	3.1	6.4	95.7
5	2	.7	1.4	97.2
6	1	.3	.7	97.9
7 or more*	3	1.0	2.1	100.0
Total	290	100.0	100.0	-----

*The three respondents in the "7 or more" category listed the following number of people as being directly responsible for computer security:

1. 10
2. 14
3. 12

percent, had the title Operations Manager, Supervisor, or Director. Sixty-two percent, or 19.2 percent, had a title other than that listed on the questionnaire. Since some of the respondents had more than one designated person, there was more than one title listed (See Tables X and XI).

Reasons for Not Having Person Directly Responsible for Computer Security (Section I-6 of Questionnaire)

Of the 149 respondents who indicated that their organization did not have a designated person directly responsible for computer security, a further analysis for the "no" answer is shown in Table XII.

Over one-third, or 35.9 percent, indicated that the computer security function is performed as part of other responsibilities and not listed as a separate job function. Nearly one-fifth of the respondents, or 19.7 percent, indicated that their organization has no formal program in computer security. Only five respondents, or 1.6 percent, indicated that consultants are utilized for computer security analysis purposes. Nearly one-half, or 42.8 percent, of the respondents indicated that other methods of computer security analysis are utilized. Of these 137 responding to the "other" category, only eight were willing to state the methods used. These "other" methods utilized are stated as follows:

1. Special security measures are employed in accordance with Federal Government Standards. Exact measures cannot be revealed.
2. Use of password when using C.R.T.
3. A separate Data Security Unit outside computer center.

TABLE X

TITLE OF PERSON(S) DIRECTLY RESPONSIBLE FOR COMPUTER SECURITY

Value	Frequency	Percent	Valid Percent	Cumulative Percent
Security Analyst	24	7.4	7.4	7.4
Operations Analyst	15	4.7	4.7	12.1
Director of Computer Security	15	3.4	3.4	15.5
Operations Manager/ Supervisor/Director	130	40.4	40.4	55.9
Data Processing or Information Systems Director/Manager	55	17.1	17.1	73.0
Data Security Manager/ Officer/Administrator/ Analyst	24	7.8	7.8	80.8
Other*	62	19.2	19.2	100.0
Total	321**	100.0	100.0	

*Other.

**Multiple responses.

TABLE XI

"OTHER" TITLES OF PERSONS DIRECTLY RESPONSIBLE FOR COMPUTER SECURITY

Title	Number
Manager, Technical Services	6
Technical Support	4
Network Manager	2
Lab Services Manager	2
Data Entry Supervisor	2
Staff Specialist	7
Controller	5
Director or Superintendent of Building and Security	6
Warehouse Manager	2
Internal Control/EDP Audit Manager	8
Quality/Standards Assurance Coordinator	4
President	3
Vice President	2
Consultant	2
Data Librarian	2
Data Communications Manager/Director	2
Director of Loss Prevention	1
Senior Research Engineer	2
Total	62

TABLE XII

REASONS FOR ORGANIZATIONS NOT HAVING DESIGNATED PERSON(S) DIRECTLY RESPONSIBLE FOR COMPUTER SECURITY

	Frequency	Percent	Valid Percent	Cumulative Percent
Computer Security function is performed as part of other responsibilities and not listed as a separate job function	115	35.9	35.9	35.9
Have no formal program in computer security	63	19.7	19.7	55.6
Consultants are utilized for computer security analysis purposes	5	1.6	1.6	57.2
Other methods of computer security analysis are utilized*	137	42.8	42.8	100.0
Total	320**	100.0	100.0	

*Other methods.

**Multiple responses.

4. Computer Security is performed as part of other responsibilities but is listed as a concurrent job function.
5. Security is the responsibility of manager; however, not in the job description.
6. Title/function assigned to a systems programmer as an additional duty.
7. Security sign or procedure used, restricting access.
8. We are a small remote job entry site to a large data center. Security staff is at data center location.

Almost 75 percent of the respondents, 73.4 percent, were in the data processing management category. Ten percent, or 29 respondents, were in the operational management category. It is interesting to note that only .7 percent, or two respondents, have the title of Security Analyst. The DPMA membership operation category B that was used for the mailing list was to include only data processing or operational management members so this selected grouping may account for the largest percentages in those two categories. There were 46 respondents in the "other" category. Their titles are somewhat varied and many of them reflect a particular industry or government operation. These "other" positional titles are as follows:

1. Systems Engineer (two responses)
2. Systems Analyst (two responses)
3. Director, Internal Audits
4. Manager, Engineering Services
5. Administrative Supervisor
6. Business System Analyst-Consultant
7. Systems Manager
8. Manager, Planning and Control
9. Data Security Management

10. Programming Supervisor
11. Project Manager
12. Office Manager
13. Assistant Manager/Analyst, Data Processing
14. Programming Specialist
15. Director of Education
16. Consultant
17. Senior Analyst
18. Chief, Program Control Branch
19. Information Systems Manager
20. Systems Analyst
21. Applications Programming Manager
22. Computer Operations Supervisor
23. Technical Staff Supervisor
24. Data Communication Manager
25. Vice President
26. Project Analyst
27. Manager/MIS Staff
28. Technical Support Manager
29. Director, Information Center
30. Systems Analyst/Programmer
31. Project Manager
32. Systems Engineer Manager
33. Manager-Systems Planning and Quality Assurance
34. Site Manager
35. Systems Administrator (Systems Support Staff Analyst)
36. Salesman of Offsite Storage of Computer Backup Media
37. Engineering Computer Services Supervisor

38. Systems Manager
39. Supervision of Administrative Application (includes operations)
40. E.D.P. Auditor
41. Systems Programming
42. Senior Systems Analyst
43. Marketing Representative
44. Corporate Director-Information Systems

Length of Time Respondent Has Been in Present Position (Section II-2 of Questionnaire)

Nearly one-third, or 30.7 percent, of the respondents have been in their present position for three to four years. Over one-fourth, or 26.6 percent, have been in their present position for more than six years. These figures indicate also that only 12.8 percent had been in their present position for less than one year (see Tables XIII and XIV).

Length of Time in Computer-Related Position (Section II-3 of Questionnaire)

Nearly three-fourths of the respondents have been in a computer-related position for more than 10 years. This high percentage reflects, no doubt, the level of the position of the respondent. Only .7 percent, or two respondents, had been in a computer related positon for less than one year (see Table XV).

Highest Educational Level of Respondent (Section II-4 of Questionnaire)

The respondents were asked to indicate their highest educational level (see Table XVI below). Nearly one-fourth, 22.1 percent, indicated

TABLE XIII

PRESENT POSITION OF RESPONDENT

Value	Frequency	Percent	Valid Percent	Cumulative Percent
Data Processing Manager	213	73.4	73.4	73.4
Operational Management	29	10.0	10.0	83.4
Security Analyst	2	.7	.7	84.1
Other	46	15.9	15.9	100.0
Total	290	100.0	100.0	

TABLE XIV

LENGTH OF TIME RESPONDENT HAS BEEN IN PRESENT POSITION

Value	Frequency	Percent	Valid Percent	Cumulative Percent
Less than 1 year	37	12.8	12.8	12.8
1 - 2 years	43	14.8	14.8	27.6
3 - 4 years	89	30.7	30.7	58.3
5 - 6 years	43	14.8	14.8	73.1
More than 6 years	77	26.6	26.6	99.7
Did not respond	1	.3	.3	100.0
Total	290	100.0	100.0	

TABLE XV

LENGTH OF TIME RESPONDENT HAS BEEN EMPLOYED IN COMPUTER-RELATED POSITION

Value	Frequency	Percent	Valid Percent	Cumulative Percent
Less than 1 year	2	.7	.7	.7
1 - 2 years	4	1.4	1.4	2.1
3 - 4 years	11	3.8	3.8	5.9
5 - 6 years	15	5.2	5.2	11.1
7 - 10 years	41	14.1	14.2	25.3
More than 10 years	215	74.1	74.7	100.0
Did not respond	2	.7	Missing	-----
Total	290	100.0	100.0	

TABLE XVI

HIGHEST EDUCATIONAL LEVEL OF RESPONDENTS

Level	Frequency	Percent	Valid Percent	Cumulative Percent
High School Graduate	13	4.5	4.5	4.5
Some College Work	64	22.1	22.1	26.7
Associate Degree	32	11.0	11.1	37.8
Vocational/Trade School Certificate	16	5.5	5.6	43.4
Bachelor's Degree	112	38.6	38.9	82.3
Master's Degree	49	16.9	17.0	99.3
Doctoral Degree	2	.7	.7	100.0
Other	2	.7	-----	-----
Total	290	100.0	100.0	

that they had some college work. Eleven percent held an associate degree. Over one-third, 38.6 percent, were awarded a Bachelor's Degree, 16.9 percent held Master's Degrees. Only two, or .7 percent, of the respondents held doctoral degrees. Two respondents, or .7 percent, listed "other" educational levels. One of these respondents indicated that the certificate was received from a two-year business school. The other respondent earned the CDP certification. The Certificate of Data Processing (CDP) according to Ralston and Reilly (1983) was,

> . . . first awarded by DPMA . . . in 1962. The CDP examination program is dedicated to the advancement of data processing and information management and to this end has established high standards based on a broad educational framework and practical knowledge (p. 493).

To further assess the educational level of the respondents, they were asked to specify their major area of study at the highest educational level. Table XVII indicates the results.

Nearly one-third, 32.1 percent, majored in business. About one-fourth, 23.1 percent, indicated a computer science or data processing major. Engineering majors comprised 5.9 percent, math majors were 8.6 percent, arts and science were 9.0 percent, and accounting majors were 8.3 percent. Twelve respondents listed other various majors, ranging from Japanese studies, English, music, to agriculture. A total of 26 respondents, or 9.0 percent, indicated an educational level but did not specify a major.

Educational or Training Areas in Computer Security (Section II-5 of Questionnaire)

Table XVIII summarizes five possible areas that the respondent has utilized to gain education or training in computer security. The

TABLE XVII

MAJOR AREA OF STUDY OF RESPONDENT

Value	Frequency	Percent	Valid Percent	Cumulative Percent
Computer Science/ Data Processing	67	23.1	25.4	25.4
Business	93	32.1	35.2	60.6
Engineering	17	5.9	6.4	67.0
Math	25	8.6	9.5	76.5
Arts and Sciences	26	9.0	9.8	86.4
Accounting	24	8.3	9.1	95.5
Other	12	4.1	4.5	100.0
Did Not Specify	26	9.0	-----	-----
Total	290	100.0	100.0	

TABLE XVIII

EDUCATIONAL OR TRAINING AREAS IN COMPUTER SECURITY UTILIZED BY RESPONDENT

Value	Frequency	Percent	Valid Percent	Cumulative Percent
Regular college courses or college extension courses	25	5.7	5.7	5.7
In-house training programs presented by a member of their organization	54	12.3	12.3	18.0
Seminars offered by other private companies and presented by a member of their staff, including vendor-sponsored seminars	114	25.9	25.9	43.9
Self-education (i.e. independent reading and study	189	42.9	42.9	86.8
No training/education in data security	58	13.2	13.2	100.0
Total	440	100.0	100.0	

largest grouping, 42.9 percent, indicated that they were self-educated, 25.9 percent indicated they attended seminars, 12.3 percent attended in-house training programs, 5.7 percent attended regular college or college extension courses. Fifty-eight, or 13.2 percent, indicated that they had no training or education in data security.

Number of Employees Presently Supervised (Section II-6 of Questionnaire)

Table XIX indicates that over one-third, 39.0 percent, of the respondents directly supervised one to five employees at the present time. Nearly one-fifth, or 19.0 percent, supervised six to 10 employees, 13.1 percent supervised 11 to 15 employees. It is interesting to note that 11.7 percent directly supervised more than 25 employees.

Memberships in Data Processing Organizations

Table XX shows that 278 of the 290 respondents currently hold memberships in DPMA. Twenty-four respondents, or 6.7 percent, are members of ACM. Only 1.7 percent are members of the Data Security Institute.

The 49 respondents who indicated that they held memberships in "other" data processing professional organizations are listed in Table XXI. Many of these organizations not identified apparently are local or regional organizations and are not listed in Ralston and Reilly's *Encyclopedia For Computer Science and Engineering*.

Familiarity With CIS Model Curricula

Table XXII shows that 85.4 percent, or 146 of the 171 respondents who responded "yes" to this question were familiar with the DPMA

TABLE XIX

NUMBER OF EMPLOYEES DIRECTLY SUPERVISED AT THE PRESENT TIME BY RESPONDENT

Value	Frequency	Percent	Valid Percent	Cummulative Percent
None	24	8.3	8.3	8.3
1 - 5	113	39.0	39.0	47.2
6 - 10	55	19.0	19.0	66.2
11 - 15	38	13.1	13.1	79.3
16 - 20	18	6.2	6.2	85.5
21 - 25	8	2.8	2.8	88.3
More than 25	34	11.7	11.7	100.0
Total	290	100.0	100.0	

TABLE XX

DATA PROCESSING PROFESSIONAL ORGANIZATION(S) IN WHICH RESPONDENT CURRENTLY HOLDS MEMBERSHIPS

Value	Frequency	Percent	Valid Percent	Cumulative Percent
DPMA	278	77.9	77.9	77.9
ACM	24	6.7	6.7	84.6
Data Security Institute	6	1.7	1.7	86.3
Other*	49	13.7	13.7	100.0
Total	357**	100.0	100.0	

*Others.

**Multiples.

TABLE XXI

OTHER DATA PROCESSING PROFESSIONAL ORGANIZATION(S) IN WHICH RESPONDENT CURRENTLY HOLDS MEMBERSHIP

Name	Frequency
Newspaper Systems Group	1
Association of Systems Management (ASM)	4
Association for Educational Data Systems (AEDS)	4
Association of Information Systems Professionals (AISP)	2
AGA/EEI Information Systems Committee	1
CODE	1
MDPA (State Organization)	1
LUBE/CUBE	1
EDP Auditors Foundation	1
Data General User's Group	1
American Management Association (AMA)	1
Institute for Certification of Computer Professionals (ICCP)	4
Guidance (New York State Organization)	1
Society for Information Management (SIM)	4
ACUTE (Local organization)	1
Association of Small Systems of Northern California	1
URISA (Local organization)	1
38 & 38 User's Group (IBM)	2
INSUA (Local organization)	1
AFCOM (Local organization)	1
APICS (Materials Related)	2
Network of Women in Computer Technology	1
ECHO	1
Wisconsin Prime User's Group	1
ADSEI	1
Communication Management Association (CMA)	1
Institute of Electronic and Electrical Engineers	2
FORUM-SINGER User's Group	1
GMIS	1
SHARE	1
AULSA	1
Chinese Computer User's Association	1
KSSA (Kentuckiana Small Systems Users)	1
Total	49

TABLE XXII

RESPONDENT'S FAMILIARITY WITH COMPUTER INFORMATION SYSTEMS MODEL CURRICULA

Value	Frequency	Percent	Valid Percent	Cumulative Percent
DPMA	146	85.4	85.4	85.4
ACM	16	9.3	9.3	94.7
Other*	9	5.3	5.3	100.0
Total	171**	100.0	100.0	

*Other.

**Multiples.

Computer Information Systems (CIS) model curriculum. If computed on the 290 respondents, 50.3 percent indicated familiarity. This 50 percent is interesting, however. Half of the DPMA members responding were at least familiar with the curriculum models.

Sixteen percent, or 9.3 percent, indicated a familiarity with the ACM model. If computed by the 290 possible respondents, the percentage falls to 5.5. The ACM model, as stated before, is generally considered more scientific and it is, therefore, not surprising that the difference in the familiarity with the models differs so markedly.

Nine respondents indicated a familiarity with other curriculum models. These findings are shown in Table XXIII.

<u>Should Computer Center Employees Possess Computer Security Knowledge (Section III-1 of Questionnaire)</u>

Table XXIV indicates that 85.5 percent of the respondents feel that computer center employees should possess some knowledge about computer security. Only 42 respondents, or 14.5 percent felt that employees did <u>not</u> need to possess security knowledge. The high response to the "yes" opinions would seem to indicate that there is a need to address the issue of computer security and determine how this knowledge may be acquired.

<u>Reasons for "No" Response to Knowledge Question (Section III-2 of Questionnaire)</u>

The 42 respondents who indicated a "no" response to the question concerning whether computer center employees should possess some

TABLE XXIII

FAMILIARITY WITH "OTHER" CIS MODEL CURRICULA

Model	Frequency
Association for Educational Data Systems (AEDS)	4
Kentuckiana Small Systems User's (KSSA)	1
EDP Auditors Foundation	1
Financial Management Society	1
CDC	1
C.O.D.E.	1
Total	9

TABLE XXIV

RESPONDENT FEELS COMPUTER CENTER EMPLOYEES SHOULD POSSESS SOME KNOWLEDGE ABOUT COMPUTER SECURITY

Value	Frequency	Percent	Valid Percent	Cumulative Percent
Yes	248	85.5	85.5	85.5
No	42	14.5	14.5	100.0
Total	290			

knowledge about computer security were then asked to indicate the reasons for the "no" response. Table XXV shows that over half, 53.5 percent, felt that computer security should be handled only by those who are directly involved in administering security programs. A smaller percent, 43.7, indicated that it is not necessary for most employees to possess security information in order to efficiently perform their jobs.

Of the two respondents who indicate "other" responses, the following reasons were given:

1. "To many people, a little knowledge is dangerous. For most people a password and a briefing on security procedures is adequate. Too much information in the hands of people who do not need it to perform their job may turn some into "hackers" which would become self-defeating."
2. "The fewer people that have knowledge in the security used, the better the security."

Best Methods to Develop Computer Security Knowledge (Section IV-2 of Questionnaire)

When querying the members concerning the best methods to develop computer security knowledge, the 248 respondents who felt that computer center employees should possess some knowledge about computer security knowledge were then asked to give their opinions concerning what methods would best develop that knowledge in the CIS curriculum.

Table XXVI shows that 39 percent felt that a complete course in computer security in addition to incorporation of computer security topics in the CIS curriculum would be best. Almost the same number, 37.2 percent, felt that incorporation of computer security topics into

TABLE XXV

REASONS FOR "NO" RESPONSE CONCERNING WHETHER COMPUTER CENTER EMPLOYEES SHOULD POSSESS SOME KNOWLEDGE ABOUT COMPUTER SECURITY

Value	Frequency	Percent	Valid Percent	Cumulative Percent
It is not necessary for most employees to possess security information in order to efficiently perform their jobs	31	43.7	43.7	43.7
Computer security should be handled only by those who are directly involved in administering security programs	38	53.5	53.5	97.2
Other	2	2.8	2.8	100.0
Total	71**	100.0	100.0	

**Multiples

TABLE XXVI

METHODS RESPONDENT FEELS WOULD BEST DEVELOP COMPUTER SECURITY KNOWLEDGE

Value	Frequency	Percent	Valid Percent	Cumulative Percent
Complete course in computer security in addition to incorporation of computer security topics in the Computer Information Systems Curriculum	113	39.0	39.0	39.0
Complete course in computer security only	20	6.9	6.9	45.9
Incorporation of computer security topics into the current courses in the Computer Ifformation Systems Curriculum only	108	37.2	37.2	83.1
Other method	7	2.4	2.4	85.5
Did not respond	42*	14.5	14.5	100.0
Total	290	100.0	100.0	

*Answered "no" in Section III-1 of questionnaire.

the current courses in the CIS curriculum ONLY would be best. Only 6.9 percent felt that a complete course only in computer security would be best.

Seven respondents indicated that other methods would best develop knowledge. These "other" responses were:

1. "Experience a compromise or loss."
2. "Information security should be stressed in all areas of a business curriculum and not just data processing."
3. "Develop a minor in complete security. One course is not enough."
4. "Also include in other management curriculums so that non-data processing people have an understanding of why it is required."
5. "In-house instruction or on-the-job training."
6. "They need to be made aware, not taught how."
7. "Awareness overview in course on data processing issues and trends."

The frequencies and percentages shown in Tables III-XXVI will be used in later sections to show relationships and comparisons.

Section II - Ranking of Topics By Mean

Using the computer security topics listed in Section IV-I of the questionnaire, the respondents were asked to rate the topics on a Likert scale from 1 - 5 by the following scale:

1. Very important
2. Important
3. Average Importance
4. Unimportant

5. Very Unimportant

The 18 topics listed (plus one for "other") were then computed to obtain a mean and standard deviation for each topic. It is important to note before discussing these means that the 1 - 5 scale was reversed in reporting the findings so that one represents the lowest and five the highest.

In order to limit the length of the discussion, the means of the top five topics were then selected for analysis. The data on the remaining 13 topics is shown in Appendix G.

Table XXVII lists the topics as they were listed on the questionnaire.

Table XXVIII then lists the topics ranked by mean to show the importance of the topic. The top five topics, ranked by mean, are shown in Table XXIX.

The "other" topics written in by the respondents are shown in Table XXX. Many of these topics are applicable to specific types of computer application and may not be considered important to the entire computer profession. Some of the topics listed could also be considered as being included in some of the titles listed, i.e., recovery could be considered in disaster protection and security conscientiousness could be considered in overview of computer security. For the sake of completeness, all "other" will be listed, however.

Section III - Rankings of Courses by Means

Using the same Likert scale, the 15 courses in the DPMA Model Curriculum for Undergraduate Computer Information Systems Education were listed. The respondents were asked to rate the importance of including elements of computer security into these courses.

TABLE XXVII

ANALYSIS OF THE IMPORTANCE OF SELECTED TOPICS THAT MIGHT BE CONSIDERED FOR INCLUSION IN THE CIS CURRICULUM RELATING TO THE TOPIC OF COMPUTER SECURITY

Topic	Mean	Standard Deviation	Minimum	Maximum	Valid N
1. Overview of computer security	4.621	.637	3.000	5.000	248
2. Company computer security programs	3.903	.968	1.000	5.000	248
3. Embezzlement: Detection and control	3.496	1.038	1.000	5.000	248
4. EDP controls and auditing	4.105	.916	1.000	5.000	248
5. Program error	3.593	.994	1.000	5.000	248
6. Operator error	3.593	.969	1.000	5.000	248
7. Programmer fraud	3.714	1.023	1.000	5.000	248
8. Operator fraud	3.669	1.039	1.000	5.000	248
9. Software protection	4.073	.915	1.000	5.000	248
10. Hardware protection	3.972	.933	1.000	5.000	248
11. Fire protection	4.040	1.037	1.000	5.000	248
12. Disaster protection	4.177	.986	1.000	5.000	248
13. Insurance against loss	3.407	1.120	1.000	5.000	248
14. Cryptographic techniques	2.734	1.035	1.000	5.000	248
15. Protection when using service bureaus	3.453	1.046	1.000	5.000	247

TABLE XXVII (Continued)

Topic	Mean	Standard Deviation	Minimum	Maximum	Valid N
16. Time-sharing protections	3.717	1.052	1.000	5.000	247
17. Protection and privacy considerations	3.774	.968	1.000	5.000	248
18. Security Software packages (i.e. RACF)	3.216	.978	1.000	5.000	245
19. Responded to "other"					

TABLE XXVIII

COMPUTER SECURITY TOPICS RANKED BY MEAN

Topic	Mean	Rank
1. Overview of computer security	4.621	1
12. Disaster protection	4.177	2
4. EDP controls and auditing	4.105	3
9. Software protection	4.073	4
11. Fire protection	4.040	5
10. Hardware protection	3.972	6
2. Company computer security programs	3.903	7
17. Protection and privacy considerations	3.774	8
16. Time-sharing protections	3.717	9
7. Programer fraud	3.714	10
8. Operator fraud	3.669	11
6. Operator error	3.593	12
5. Program error	3.593	12
3. Embezzlement: detection and control	3.496	13
15. Protection when using service bureaus	3.453	14
13. Insurance against loss	3.407	15
18. Security software packages	3.216	16
14. Cryptographic techniques	2.734	17

TABLE XXIX

TOP FIVE COMPUTER SECURITY TOPICS, RANKED BY MEAN

Topic	Mean	Rank
1. Overview of computer security	4.621	1
12. Disaster protection	4.177	2
4. EDP controls and audit	4.105	3
9. Software protection	4.073	4
11. Fire protection	4.040	5

TABLE XXX

"OTHER" COMPUTER SECURITY TOPICS,
SUPPLIED BY THE RESPONDENT

Topic	Frequency
1. Security conscientiousness	1
2. Physical security - including clearances and controls	1
3. Phone line protection	1
4. Communication-options and risks associated with each	2
5. Risk assessment	1
6. Personal safety and security	2
7. Legal issues and considerations	2
8. Application programming techniques to support a security program	1
9. Back-up	2
10. Documentation	1
11. Disaster	2
12. Awareness of the need for security	1
13. Cost of security (having it verses not having it)	1
14. Network security	1
Total	19

The same Likert scale used in rating the topics above was utilized. The one to five scale was again reversed, as was done with the topics, so that one represents "very unimportant" and five represents "very important."

The means of the courses are given in Table XXXI, listed in order of CIS number. Table XXXII lists the courses, ranked by mean. Table XXXIII lists the top five courses, ranked by mean. To limit the length of the comparative analysis of the data, only the top five courses will be used. The data for the other 10 courses is shown in Appendix I.

Section IV - Cross Tabulations of Topics and Courses

The top five topics chosen by means to be analyzed are:

1. Overview of computer security
2. Disaster protection
3. EDP controls and auditing
4. Software protection
5. Fire protection

The statistical summaries for the additional topics not shown here are listed in Appendix H for reference.

The top five CIS courses chosen by means to be analyzed are:

1. CIS-13 EDP Audit and Controls
2. CIS-6 Database Program Development
3. CIS-7 Applied Software Development Project
4. CIS-12 Distributed Data Processing
5. CIS-15 Information Resource Management

The statistical summaries for the additional courses not shown here are listed in Appendix I for reference.

TABLE XXXI

ANALYSIS OF IMPORTANCE OF INCLUDING ELEMENTS OF COMPUTER SECURITY INTO CIS COURSES

Course	Mean	Standard Deviation	Minimum	Maximum	Valid N
Core Courses					
CIS-1	3.534	1.147	1.000	6.000	247
CIS-2	3.077	1.060	1.000	5.000	248
CIS-3	3.423	.999	1.000	5.000	248
CIS-4	3.806	.956	1.000	5.000	247
CIS-5	3.773	1.023	1.000	5.000	247
CIS-6	4.016	.915	1.000	5.000	247
CIS-7	3.942	.992	1.000	5.000	242
Elective Courses					
CIS-8	3.453	.951	1.000	5.000	245
CIS-9	3.427	1.019	1.000	5.000	246
CIS-10	3.465	.998	1.000	5.000	245
CIS-11	3.813	1.013	1.000	5.000	246
CIS-12	3.911	.986	1.000	5.000	246
CIS-13	4.484	.846	1.000	5.000	246
CIS-14	3.769	.958	1.000	5.000	247
CIS-15	3.834	.950	1.000	5.000	247

TABLE XXXII

ANALYSIS OF IMPORTANCE OF INCLUDING ELEMENTS OF COMPUTER SECURITY INTO CIS COURSES RANKED BY MEAN

Course Title	Mean	Rank
CIS-13 EDP Audit and Controls	4.484	1
CIS-6 Database Program Development	4.016	2
CIS-7 Applied Software Development Project	3.942	3
CIS-12 Distributed Data Processing	3.911	4
CIS-15 Information Resource Management	3.834	5
CIS-11 Advanced Database Concepts	3.813	6
CIS-4 Systems Analysis Methods	3.806	7
CIS-5 Structured Systems Analysis and Design	3.773	8
CIS-14 Information Systems Planning	3.769	9
CIS-1 Introduction to Computer-based Systems	3.534	10
CIS-10 Decision Support Systems	3.465	11
CIS-8 Software and Hardware Concepts	3.453	12
CIS-9 Office Automation	3.427	13
CIS-3 Applications Program Development II	3.423	14
CIS-2 Applications Program Development I	3.077	15

TABLE XXXIII

LISTING OF TOP FIVE COURSES FOR INCLUSION OF COMPUTER SECURITY TOPICS

Courses	Mean	Rank
CIS-13 EDP Audit and Controls	4.484	1
CIS-6 Database Program Development	4.016	2
CIS-7 Applied Software Development Project	3.942	3
CIS-12 Distributed Data Processing	3.911	4
CIS-15 Information Resource Management	3.834	5

Table XXXIV shows that when comparing the top five topics to the number of employees in the respondent's computer center, the highest mean on the one to five scale is 4.8000 in the 41 - 60 employee category for topic one. The highest mean, 4.3243, for Topic Two is in the 21 - 40 category. The highest mean for Topic Three is in the 61 - 80 category 4.3333. The highest mean in Topic Four is in the 21 - 40 category, 4.2973. The highest mean in Topic Five is in the 21 - 40 category, 4.1892. The categories are shown together in Table XXXV.

Tables XXXVI and XXXVII show a breakdown of the top five topics compared to whether the respondent's computer center had a designated person directly responsible for computer security. The missing cases indicate that 42 respondents did not respond to this question. Of the 248 respondents who did respond, the largest overall mean was in Topic One - Security Overview, with "yes" as 4.6480, "no" represented by 4.5935, and an overall mean of 4.6210.

Tables XXXVIII and XXXIX show the breakdown when comparing individual top five topics to the number of designated security persons in the respondent's computer center. Again, the largest mean is shown in Topic One - Security Overview with an overall mean of 4.6720. The 165 missing cases indicate that the respondent did not have a designated person and, therefore, did not respond to the question. These figures represent only those 125 persons who indicated in the previous question a "yes" response.

Tables XXXX and XXXXI show that when comparing the individual top five topics to the respondent's present position, again Topic One - Security Overview, has the highest mean, 4.6210. The missing 42 are representative of those who indicated in an earlier response that their computer center did not have a designated person responsible for computer security.

TABLE XXXIV

COMPARING INDIVIDUAL TOP FIVE TOPICS
TO NUMBER OF EMPLOYEES

Number of Employees	Mean	Std Dev	Cases
	Topic 1 - Security Overview		
	4.6210	.6375	248
1 - 20	4.6357	.6141	140
21 - 40	4.4054	.7979	37
41 - 60	4.8000	.4104	20
61 - 80	4.6667	.5164	6
81 - 100	4.6923	.6304	13
Over 100	4.6563	.6530	32
Total Cases = 290			
Missing Cases = 42 or 14.5 PCT.			
	Topic 2 - Disaster Protection		
	4.1774	.9861	248
1 - 20	4.2071	.9407	140
21 - 40	4.3243	.8836	37
41 - 60	4.3000	.8013	20
61 - 80	4.1667	.9832	6
81 - 100	4.0000	1.2910	13
Over 100	3.8750	1.2378	32
Total Cases = 290			
Missing Cases = 42 or 14.5 PCT.			
	Topic 3 - EDP Controls and Auditing		
	4.1048	.9161	248
1 - 20	4.0357	.9400	140
21 - 40	4.3243	.7474	37
41 - 60	4.2500	.9665	20
61 - 80	4.3333	.8165	6
81 - 100	4.1538	.8006	13
Over 100	4.0000	1.0160	32
Total Cases = 290			
Missing Cases = 42 or 14.5 PCT.			

TABLE XXXIV (Continued)

Number of Employees	Mean	Std Dev	Cases
	Topic 4 - Software Protection		
	4.0726	.9148	248
1 - 20	4.0786	.9450	140
21 - 40	4.2973	.8119	37
41 - 60	3.8500	.9333	20
61 - 80	3.6667	.8165	6
81 - 100	4.0769	.9541	13
Over 100	4.0000	.8799	32
Total Cases = 290			
Missing Cases = 42 or 14.5 PCT.			
	Topic 5 - Fire Protection		
	4.0403	1.0370	248
1 - 20	4.1000	1.0199	140
21 - 40	4.1892	.9672	37
41 - 60	4.1000	.7881	20
61 - 80	3.6667	1.2111	6
81 - 100	3.7692	1.3009	13
Over 100	3.7500	1.1640	32
Total Cases = 290			
Missing Cases = 42 or 14.5 PCT.			

TABLE XXXV

TOP FIVE TOPICS COMPARED TO NUMBER OF EMPLOYEES IN COMPUTER CENTER

Number of Employees	Security Overview	Disaster Protection	EDP Controls and Auditing	Software Protection	Fire Protection
1 - 20	4.6357	4.2071	4.0357	4.0786	4.1000
21 - 40	4.4054	4.3243	4.3243	4.2973	4.1892
41 - 60	4.8000	4.3000	4.2500	4.8500	4.1000
61 - 80	4.6667	4.1667	4.3333	4.6667	3.6667
81 - 100	4.6923	4.0000	4.1538	4.0769	3.7692
Over 100	4.6563	3.8750	4.0000	4.000	3.7500

TABLE XXXVI

COMPARING INDIVIDUAL TOP FIVE TOPICS TO PRESENCE OF DESIGNATED SECURITY PERSON

	Mean	Std Dev	Cases
	Topic 1 - Security Overview		
	4.6210	.6375	248
Yes	4.6480	.6255	125
No	4.5935	.6508	123
Total Cases = 290			
Missing Cases = 42 or 14.5 PCT.			
	Topic 2 - Disaster Protection		
	4.1774	.9861	248
Yes	4.1280	1.0699	125
No	4.2276	.8945	123
Total Cases = 290			
Missing Cases = 42 or 14.5 PCT.			
	Topic 3 - EDP Controls and Auditing		
	4.1048	.9161	248
Yes	4.0506	.9445	125
No	4.1545	.8874	123
Total Cases = 290			
Missing Cases = 42 or 14.5 PCT.			
	Topic 4 - Software Protection		
	4.0726	.9148	248
Yes	4.1520	.8619	125
No	3.9919	.9624	123
Total Cases = 290			
Missing Cases = 42 or 14.5 PCT.			

TABLE XXXVI (Continued)

	Mean	Std Dev	Cases
	Topic 5 - Fire Protection		
	4.0403	1.0370	248
Yes	4.0160	1.1070	125
No	4.0650	.9644	123

Total Cases = 290

Missing Cases = 42 or 14.5 PCT.

TABLE XXXVII

TOP FIVE TOPICS COMPARED TO PRESENCE OF DESIGNATED SECURITY PERSON

Designated Security Person	Security Overview	Disaster Protection	EDP Controls and Auditing	Software Protection	Fire Protection
Yes	4.6480	4.1280	4.0560	4.1520	4.0160
No	4.5935	4.2276	4.1545	3.9919	4.0650

TABLE XXXVIII

COMPARING INDIVIDUAL TOP FIVE TOPICS TO NUMBER OF DESIGNATED SECURITY PERSONS

	Mean	Std Dev	Cases
	Topic 1 - Security Overview		
	4.6720	.6061	125
1	4.6034	.6196	58
2	4.7073	.5587	41
3	4.6667	.7785	12
4	4.7778	.6667	9
5	5.0000	.0000	2
6	5.0000	.0000	1
7	5.0000	.0000	2

Total Cases = 290
Missing Cases = 165 or 56.9 PCT.

	Mean	Std Dev	Cases
	Topic 2 - Disaster Protection		
	4.1440	1.0754	125
1	4.2241	1.0603	58
2	4.1463	1.0854	41
3	4.5833	.6686	12
4	3.2222	1.0929	9
5	3.5000	2.1213	2
6	3.0000	.0000	1
7	4.5000	.7071	2

Total Cases = 290
Missing Cases = 165 or 56.9 PCT.

	Mean	Std Dev	Cases
	Topic 3 - EDP Controls and Auditing		
	4.0320	.9413	125
1	4.1207	.8801	58
2	4.0000	.8944	41
3	4.0000	1.0445	12
4	3.8889	1.0541	9
5	4.0000	1.4142	2
6	1.0000	.0000	1
7	4.5000	.7071	2

Total Cases = 290
Missing Cases = 165 or 56.9 PCT.

TABLE XXXVIII (Continued)

	Mean	Std Dev	Cases
	Topic 4 - Software Protection		
	4.1440	.8586	125
1	4.0517	.9986	58
2	4.2195	.7250	41
3	4.2500	.6216	12
4	4.1111	.7817	9
5	4.0000	1.4142	2
6	4.0000	.0000	1
7	5.0000	.0000	2
Total Cases = 290			
Missing Cases = 165 or 56.9 PCT.			
	Topic 5 - Fire Protection		
	4.0480	1.1061	125
1	4.0862	1.0807	58
2	4.0000	1.2247	41
3	4.5000	.6742	12
4	3.3333	.8660	9
5	3.5000	2.1213	2
6	4.0000	.0000	1
7	5.000	.0000	2
Total Cases = 290			
Missing Cases = 165 or 56.9 PCT.			

TABLE XXXIX

TOP FIVE TOPICS COMPARED TO NUMBER OF DESIGNATED SECURITY PERSONS

Designated Security Person	Security Overview	Disaster Protection	EDP Controls and Auditing	Software Protection	Fire Protection
1	4.6034	4.2241	4.1207	4.0517	4.0862
2	4.7073	4.1463	4.0000	4.2195	4.0000
3	4.6667	4.5833	4.0000	4.2500	4.5000
4	4.7778	3.2222	3.8889	4.1111	3.3333
5	5.0000	3.5000	4.0000	4.0000	3.5000
6	5.0000	3.0000	1.0000	4.0000	4.0000
7 or more	5.0000	4.5000	4.5000	5.0000	5.0000

TABLE XXXX

COMPARING INDIVIDUAL TOP FIVE TOPICS TO PRESENT POSITION OF RESPONDENT

Position	Mean	Std Dev	Cases
	Topic 1 - Security Overview		
	4.6210	.6375	248
Data Processing Management	4.5989	.6637	182
Operational Management	4.6154	.6373	26
Security Analyst	5.0000	.0000	2
OTHER	4.7105	.5151	38

Total Cases = 290

Missing Cases = 42 or 14.5 PCT.

Position	Mean	Std Dev	Cases
	Topic 2 - Disaster Protection		
	4.1774	.9861	248
Data Processing Management	4.1593	.9927	182
Operational Management	4.5385	.7606	26
Security Analyst	2.0000	1.4142	2
OTHER	4.1316	.9349	38

Total Cases = 290

Missing Cases = 42 or 14.5 PCT.

Position	Mean	Std Dev	Cases
	Topic 3 - EDP Controls and Auditing		
	4.1048	.9161	248
Data Processing Management	4.1209	.9022	182
Operational Management	4.0769	.9348	26
Security Analyst	4.5000	.7071	2
OTHER	4.0263	.9996	38

Total Cases = 290

Missing Cases = 42 or 14.5 PCT.

TABLE XXXX (Continued)

Positions	Mean	Std Dev	Cases
	Topic 4 - Software Protection		
	4.0726	.9148	248
Data Processing Management	4.0549	.9503	182
Operational Management	4.1154	.8162	26
Security Analyst	3.5000	.7071	2
OTHER	4.1579	.8229	38
Total Cases = 290			
Missing Cases = 42 or 14.5 PCT.			
	Topic 5 - Fire Protection		
	4.0403	1.0370	248
Data Processing Management	4.0385	1.0319	182
Operational Management	4.2308	.9081	26
Security Analyst	2.0000	1.4142	2
OTHER	4.0263	1.0523	38
Total Cases = 290			
Missing Cases = 42 or 14.5 PCT.			

TABLE XXXXI

TOP FIVE TOPICS COMPARED TO RESPONDENT'S PRESENT POSITION

Present Position	Security Overview	Disaster Protection	EDP Controls and Auditing	Software Protection	Fire Protection
Data Processing Management	4.5989	4.1593	4.1209	4.0549	4.0385
Operational Management	4.6154	4.5385	4.0769	4.1154	4.2308
Security Analyst	5.0000	2.0000	4.5000	3.5000	2.0000
Other	4.7105	4.1316	4.0263	4.1579	4.0263

Tables XXXXII and XXXXIII show that when comparing the top five topics to the respondents' time at their present position, the highest mean is again shown in Topic One - Security Overview. The 42 missing cases represent those respondents who do not have a designated security person in their computer center.

Tables XXXXIV and XXXXV compare the individual top five topics to the length of time the respondent has been in a computer-related position. The 44 respondents shown in missing failed to answer this question. The highest mean was again shown in Topic One - Security Overview, 4.6179.

Tables XXXXVI and XXXXVII compare the individual top five topics to the highest educational level of the respondent. The 44 responses missing are the result of respondent's who failed to complete this question. The highest mean is again recorded in the Security Overview Topic, 4.6179.

Breakdown by Courses

Tables XXXXVIII and XXXXIX compare the number of employees in the respondent's computer center to the individual top five courses in the CIS curriculum. The highest mean, 4.4837, is in the CIS-13 category. The highest individual mean of 4.8333 is contained in the 61 - 80 category in this same course. The missing numbers represent either those who did not respond due to a "no" response to Section III-1 of the questionnaire or the fact that the respondent merely failed to rate all the categories listed.

Tables L and LI show that respondents whose computer centers have a designated person directly responsible for computer security tended to rate the topics slightly higher than those who did not have a designated

TABLE XXXXII

COMPARING INDIVIDUAL TOP FIVE TOPICS TO RESPONDENT'S TIME AT PRESENT POSITION

Topic	Mean	Std Dev	Cases
Topic 1 - Security Overview			
	4.6210	.6375	248
Less 1 year	4.5455	.7111	33
1 - 2 years	4.5882	.6089	34
3 - 4 years	4.6623	.5761	77
5 - 6 years	4.7250	.5057	40
Over 6 years	4.5556	.7573	63
Did not respond	5.0000	.0000	1
Total Cases = 290			
Missing Cases = 42 or 14.5 PCT.			
Topic 2 - Disaster Protection			
	4.1774	.9861	248
Less 1 year	4.1818	.9505	33
1 - 2 years	3.9706	1.0867	34
3 - 4 years	4.3247	.9381	77
5 - 6 years	4.3000	.8533	40
Over 6 years	4.0794	1.0049	63
Did not respond	1.0000	.0000	1
Total Cases = 290			
Missing Cases = 42 or 14.5 PCT.			
Topic 3 - EDP Controls and Auditing			
	4.1048	.9161	248
	4.1818	.9170	33
Less 1 year	4.0588	1.0714	34
1 - 2 years	4.1948	.7954	77
3 - 4 years	4.2000	.7579	40
5 - 6 years	3.9048	1.0429	63
Over 6 years	5.0000	.0000	1
Did not respond			
Total Cases = 290			
Missing Cases = 42 or 14.5 PCT.			

TABLE XXXXII (Continued)

Topic	Mean	Std Dev	Cases
	Topic 4 - Software Protection		
	4.0726	.9148	248
Less 1 year	3.7879	.9924	33
1 - 2 years	3.8824	.9460	34
3 - 4 years	4.1818	.8695	77
5 - 6 years	4.0000	.8165	40
Over 6 years	4.2540	.9327	63
Did not respond	3.0000	.0000	1
Total Cases = 290			
Missing Cases = 42 or 14.5 PCT.			
	Topic 5 - Fire Protection		
	4.0403	1.0370	248
Less 1 year	3.9697	.9515	33
1 - 2 years	3.8529	1.1582	34
3 - 4 years	4.1948	.9739	77
5 - 6 years	4.2000	.8533	40
Over 6 years	3.9365	1.1198	63
Did not respond	1.0000	.0000	1
Total Cases = 290			
Missing Cases = 42 or 14.5 PCT.			

TABLE XXXXIII

TOP FIVE TOPICS COMPARED TO RESPONDENT'S LENGTH OF TIME IN PRESENT POSITION

Length of Time	Security Overview	Disaster Protection	EDP Controls and Auditing	Software Protection	Fire Protection
Less than one year	4.5455	4.1818	4.1818	3.7879	3.9697
1 - 2 years	4.5882	3.9706	4.0588	3.8824	3.8529
3 - 4 years	4.6623	4.3247	4.1948	4.1818	4.1948
5 - 6 years	4.7250	4.3000	4.2000	4.0000	4.2000
Over 6 years	4.5556	4.0794	3.9048	4.2540	3.9365

TABLE XXXXIV

COMPARING INDIVIDUAL TOP FIVE TOPICS TO LENGTH OF TIME RESPONDENT HAS BEEN IN A COMPUTER-RELATED POSITION

Topic	Mean	Std Dev	Cases
Topic 1 - Security Overview			
	4.6179	.6391	246
Less 1 year	5.0000	.0000	1
1 - 2 years	5.0000	.0000	2
3 - 4 years	4.7143	.7559	7
5 - 6 years	4.7692	.4385	13
7 - 10 years	4.6857	.5827	35
Over 10 years	4.5851	.6607	188
Total Cases = 290			
Missing Cases = 44 or 15.2 PCT.			
Topic 2 - Disaster Protection			
	4.1870	.9676	246
Less 1 year	5.0000	.0000	1
1 - 2 years	5.0000	.0000	2
3 - 4 years	4.2857	1.1127	7
5 - 6 years	4.2308	1.0127	13
Over 6 years	4.1429	.9438	35
Did not respond	4.1755	.9735	188
Total Cases = 290			
Missing Cases = 44 or 15.2 PCT.			
Topic 3 - EDP Controls and Auditing			
	4.1057	.9153	246
	3.0000	.0000	1
Less 1 year	4.0000	.0000	2
1 - 2 years	4.0000	1.0000	7
3 - 4 years	4.0000	1.1547	13
5 - 6 years	4.0571	.9375	35
Over 6 years	4.1330	.9006	188
Did not respond			
Total Cases = 290			
Missing Cases = 44 or 15.2 PCT.			

TABLE XXXXIV (Continued)

Topic	Mean	Std Dev	Cases
	Topic 4 - Software Protection		
	4.0772	.9159	246
Less 1 year	4.0000	.0000	1
1 - 2 years	5.0000	.0000	2
3 - 4 years	4.2857	.9512	7
5 - 6 years	4.3846	.7679	13
7 - 10 years	4.0857	.8869	35
Over 10 years	4.0372	.9329	188
Total Cases = 290			
Missing Cases = 44 or 15.2 PCT.			
	Topic 5 - Fire Protection		
	4.0488	1.0210	246
Less 1 year	4.0000	.0000	1
1 - 2 years	5.0000	.0000	2
3 - 4 years	4.4286	.9759	7
5 - 6 years	3.9231	1.0377	13
7 - 10 years	3.9714	.9848	35
Over 10 years	4.0479	1.0356	188
Total Cases = 290			
Missing Cases = 44 or 15.2 PCT.			

TABLE XXXXV

TOP FIVE TOPICS COMPARED TO LENGTH OF TIME RESPONDENT HAS BEEN IN COMPUTER-RELATED POSITION

Length of Time	Security Overview	Disaster Protection	EDP Controls and Auditing	Software Protection	Fire Protection
Less than one year	5.0000	5.0000	3.0000	4.0000	4.0000
1 - 2 years	5.0000	5.0000	4.0000	5.0000	5.0000
3 - 4 years	4.7143	4.2857	4.0000	4.2857	4.4286
5 - 6 years	4.7692	4.2308	4.0000	4.3846	3.9231
7 - 10 years	4.6857	4.1429	4.0571	4.0857	3.9714
Over 10 years	4.5851	4.1755	4.1330	4.0372	4.0479

TABLE XXXXVI

COMPARING INDIVIDUAL TOP FIVE TOPICS TO HIGHEST EDUCATIONAL LEVEL OF RESPONDENT

Topic	Mean	Std Dev	Cases
Topic 1 - Security Overview			
	4.6179	.6391	246
High School Graduate	4.5556	.7265	9
Some College	4.5556	.6914	54
Associate Degree	4.5926	.6360	27
Vocational/Technical School Certificate	4.4167	.7930	12
Bachelor's Degree	4.6733	.6018	101
Master's Degree	4.6429	.6177	42
Doctoral Degree	5.0000	.0000	1
Total Cases = 290			
Missing Cases = 44 or 15.2 PCT.			
Topic 2 - Disaster Protection			
	4.1789	.9859	246
High School Graduate	4.3333	.7071	9
Some College	4.2963	.8385	54
Associate Degree	4.3333	.6794	27
Vocational/Technical School Certificate	4.5833	.6686	12
Bachelor's Degree	4.0594	1.1298	101
Master's Degree	4.0952	1.0548	42
Doctoral Degree	3.0000	.0000	1
Total Cases = 290			
Missing Cases = 44 or 15.2 PCT.			
Topic 3 - EDP Controls and Auditing			
	4.1098	.9170	246
High School Graduate	4.2222	.9718	9
Some College	4.2407	.8673	54
Associate Degree	4.0370	.7061	27
Vocational/Technical School Certificate	4.5833	.5149	12
Bachelor's Degree	4.0891	.9066	101
Master's Degre	3.8571	1.1385	42
Doctoral Degree	5.0000	.0000	1
Total Cases = 290			
Missing Cases = 44 or 15.2 PCT.			

TABLE XXXXVI (Continued)

Topic	Mean	Std Dev	Cases
	Topic 4 - Software Protection		
	4.0691	.9166	246
High School Graduate	4.1111	.7817	9
Some College	4.2037	.8770	54
Associate Degree	4.1111	.8473	27
Vocational/Technical School Certificate	4.0000	1.1282	12
Bachelor's Degree	3.9505	.9734	101
Master's Degree	4.1429	.8431	42
Doctoral Degree	5.0000	.0000	1
Total Cases = 290			
Missing Cases = 44 or 15.2 PCT.			
	Topic 5 - Fire Protection		
	4.0447	1.0391	246
High School Graduate	4.4444	.7265	9
Some College	4.2222	.8615	54
Associate Degree	4.1852	.8338	27
Vocational/Technical School Certificate	4.5833	.6686	12
Bachelor's Degree	3.8713	1.1888	101
Master's Degree	3.9286	1.0451	42
Doctoral Degree	3.0000	.0000	1
Total Cases = 290			
Missing Cases = 44 or 15.2 PCT.			

TABLE XXXXVII

TOP FIVE TOPICS COMPARED TO HIGHEST EDUCATIONAL LEVEL OF RESPONDENT

Highest Education Level	Security Overview	Disaster Protection	EDP Controls and Auditing	Software Protection	Fire Protection
High School Graduate	4.5556	4.3333	4.2222	4.1111	4.4444
Some College	4.5556	4.2963	4.2407	4.2037	4.2222
Associate Degree	4.5926	4.3333	4.0370	4.1111	4.1852
Vocational/ Trade School Certificate	4.4167	4.5833	4.5833	4.0000	4.5833
Bachelor's Degree	4.6733	4.0594	4.0891	3.9505	3.8713
Master's Degree	4.6429	4.0952	3.8571	4.1429	3.9286
Doctoral Degree	5.0000	3.0000	5.0000	5.0000	3.0000

TABLE XXXXVIII

NUMBER OF EMPLOYEES IN RESPONDENT'S COMPUTER CENTER COMPARED TO TOP FIVE CIS COURSES

Number	Mean	Std Dev	Cases
	CIS-13		
	4.4837	.8462	246
1 - 20	4.5108	.8285	139
21 - 40	4.4444	.8433	36
41 - 60	4.5000	.6882	20
61 - 80	4.8333	.4082	6
81 - 100	4.3077	.9473	13
Over 100	4.4063	1.0429	32
Total Cases = 290			
Missing Cases = 44 or 15.2 PCT.			
	CIS-6		
	4.0162	.9150	247
1 - 20	4.0072	.9207	139
21 - 40	4.2432	.6833	37
41 - 60	3.9000	.9679	20
61 - 80	4.0000	.8944	6
81 - 100	3.6923	1.0316	13
Over 100	4.0000	1.0473	32
Total Cases = 290			
Missing Cases = 43 or 14.8 PCT.			
	CIS-7		
	3.9421	.9921	242
1 - 20	3.9493	1.0416	138
21 - 40	4.0833	.7700	36
41 - 60	3.8421	.9582	19
61 - 80	4.1667	.9832	6
81 - 100	3.5000	1.0000	12
Over 100	3.9355	1.0307	31
Total Cases = 290			
Missing Cases = 48 or 16.6 PCT.			

TABLE XXXXVIII (Continued)

Number	Mean	Std Dev	Cases
	CIS-12		
	3.9106	.9857	246
1 - 20	3.8993	1.0165	139
21 - 40	3.8056	1.0370	36
41 - 60	4.1000	.8522	20
61 - 80	3.6667	1.0328	6
81 - 100	4.0769	.9541	13
Over 100	3.9375	.9136	32
Total Cases = 290			
Missing Cases = 44 or 15.2 PCT.			
	CIS-15		
	3.8340	.9504	247
1 - 20	3.8345	.9525	139
21 - 40	4.0270	.9856	37
41 - 60	3.7500	1.0699	20
61 - 80	3.8333	.9832	6
81 - 100	3.7692	.7250	13
Over 100	3.6875	.9311	32
Total Cases = 290			
Missing Cases = 43 or 14.8 PCT.			

TABLE XXXXIX

BREAKDOWN OF NUMBER OF EMPLOYEES IN RESPONDENT'S COMPUTER CENTER COMPARED TO TOP FIVE CIS COURSES

	CIS-13	CIS-6	CIS-7	CIS-12	CIS-15
1 - 20	4.5108	4.0072	3.9493	3.8993	3.8345
21 - 40	4.4444	4.2432	4.0833	3.8056	4.0270
41 - 60	4.5000	3.9000	3.8421	4.1000	3.7500
61 - 80	4.8333	4.0000	4.1667	3.6667	3.8333
81 - 100	4.3077	3.6923	3.5000	4.0769	3.7692
Over 100	4.4063	4.0000	3.9355	3.9375	3.6875

TABLE L

INDIVIDUAL TOP FIVE TOPICS COMPARED TO WHETHER RESPONDENT'S COMPUTER CENTER HAS A DESIGNATED SECURITY PERSON

Response	Mean	Std Dev	Cases
	CIS-13		
	4.4837	.8462	246
Yes	4.4355	.8948	124
No	4.5328	.7944	120
Total Cases = 290			
Missing Cases = 44 or 15.2 PCT.			
	CIS-6		
	4.0162	.9150	247
Yes	4.0726	.9298	124
No	3.9593	.8999	123
Total Cases = 290			
Missing Cases = 43 or 14.8 PCT.			
	CIS-7		
	3.9421	.9921	242
Yes	4.0083	.9958	121
No	3.8760	.8980	121
Total Cases = 290			
Missing Cases = 48 or 16.6 PCT.			
	CIS-12		
	3.9106	.9857	246
Yes	3.9113	.9196	124
No	3.9098	1.0524	122
Total Cases = 290			
Missing Cases = 44 or 15.2 PCT.			
	CIS-15		
	3.8340	.9504	247
Yes	3.8871	.9389	124
No	3.7805	.9627	123
Total Cases = 290			
Missing Cases = 43 or 14.8 PCT.			

TABLE LI

BREAKDOWN OF INDIVIDUAL TOP FIVE TOPICS COMPARED TO WHETHER RESPONDENT'S COMPUTER CENTER HAS A DESIGNATED SECURITY PERSON

	CIS-13	CIS-6	CIS-7	CIS-12	CIS-15
Yes	4.4358	4.0726	4.0083	3.9113	3.8871
No	4.5328	3.9593	3.8760	3.9098	3.7805

person. CIS-13 again showed the highest mean, 4.4837, as well as the highest means for the yes and no responses, 4.4355 and 4.5328.

Tables LII and LIII show that CIS-13 generally contains higher means, except for the seven or more categories. The missing numbers represent those respondents who indicated that they did not have a designated person and, therefore, did not respond to this question.

Tables LIV and LV show the highest overall mean in CIS-13. The Data Processing Management position generally shows higher means than the other two categories. Part of this is due to a considerably larger number of respondents, 181 compared to only 26 in Operational Management.

Tables LVI and LVII show that CIS-13 has the highest mean. The means shown in the tables tend to vary in respect to length of time respondent has been in present position with the different courses. As an example, CIS-13 showed the highest mean in the one to two year category, CIS-6 showed the highest mean in the over six year category, CIS-7 showed the highest mean in the three to four year category, CIS-12 in the over six year category, CIS-15 in the five to six year category.

Tables LVIII and LIX show that the highest overall mean is in the CIS-13 course. The category of three to four years generally shows higher means for all five courses. The lowest means tend to be in the one to two year category throughout.

Tables LX and LXI show that highest overall mean is in the CIS-13 course, 4.4836. The other highest means were not clustered and tended to vary with the individual courses. CIS-13's highest mean was in the vocational-technical school category. CIS-6's highest mean was in the Bachelor's category. CIS-7's category was in the high school and Associate degree category. CIS-12's highest mean was in the high school

TABLE LII

INDIVIDUAL COURSES COMPARED TO NUMBER OF PEOPLE DIRECTLY RESPONSIBLE FOR COMPUTER SECURITY IN RESPONDENT'S COMPUTER CENTER

	Mean	Std Dev	Cases
	CIS-13		
	4.4320	.9362	125
1	4.4655	.9591	58
2	4.3902	.9455	41
3	4.2500	1.1382	12
4	4.6667	.5000	9
5	5.0000	.0000	2
6	5.0000	.0000	1
7 or more	3.5000	.7071	2
Total Cases = 290			
Missing Cases = 165 or 56.9 PCT.			
	CIS-6		
	4.1040	.9230	125
1	4.0862	.9231	58
2	4.1463	.9370	41
3	4.0000	.8728	12
4	4.0000	1.1180	9
5	4.5000	.7071	2
6	3.0000	.0000	1
7 or more	5.0000	.0000	2
Total Cases = 290			
Missing Cases = 165 or 56.9 PCT.			
	CIS-7		
	4.0082	.9917	122
1	3.9825	1.0937	57
2	4.0256	.9594	39
3	3.9167	.9003	12
4	4.2222	.8333	9
5	4.5000	.7071	2
6	3.0000	.0000	1
7 or more	4.0000	.0000	2
Total Cases = 290			
Missing Cases = 165 or 57.9 PCT.			

TABLE LII (Continued)

	Mean	Std Dev	Cases
		CIS-12	
	3.9040	.9624	125
1	3.8621	1.0165	58
2	3.7561	.9160	41
3	4.2500	.7538	12
4	4.1111	1.1667	9
5	4.5000	.7071	2
6	4.0000	.0000	1
7 or more	4.5000	.7071	2
Total Cases = 290			
Missing Cases = 165 or 56.9 PCT.			
		CIS-15	
	3.8800	.9384	125
1	3.9138	.9784	58
2	3.8293	.8917	41
3	3.8333	1.1146	12
4	4.1111	.6009	9
5	4.0000	1.4142	2
6	4.0000	.0000	1
7 or more	3.0000	1.4142	2
Total Cases = 290			
Missing Cases = 165 or 56.9 PCT.			

TABLE LIII

BREAKDOWN OF INDIVIDUAL COURSES COMPARED TO NUMBER OF PEOPLE DIRECTLY RESPONSIBLE FOR COMPUTER SECURITY AT RESPONDENT'S COMPUTER CENTER

	CIS-13	CIS-6	CIS-7	CIS-12	CIS-15
1	4.4655	4.0862	3.9825	3.8621	3.9138
2	4.3902	4.1463	4.0256	3.7561	3.8293
3	4.2500	4.0000	3.9167	4.2500	3.8333
4	4.6667	4.0000	4.2222	4.1111	4.1111
5	5.0000	4.5000	4.5000	4.5000	4.0000
6	5.0000	3.0000	3.0000	4.0000	4.0000
7 or more	3.5000	5.0000	4.0000	4.5000	3.0000

TABLE LIV

TOP FIVE COURSES COMPARED TO RESPONDENT'S PRESENT POSITION

	Mean	Std Dev	Cases
	CIS-13		
	4.4837	.8462	246
Data Processing Management	4.4807	.8339	181
Operational			26
Management	4.3077	.8840	2
Security Management	3.0000	2.8284	37
Other	4.7027	.6610	
Total Cases = 290			
Missing Cases = 44 or 15.2 PCT.			
	CIS-6		
	4.0162	.9150	247
Data Processing Management	4.0331	.9244	181
Operational Management	3.9615	.7736	26
Security Management	2.5000	2.1213	2
Other	4.0526	.8683	38
Total Cases = 290			
Missing Cases = 43 or 14.8 PCT.			
	CIS-7		
	3.9421	.9921	242
Data Processing Management	3.9266	1.0114	177
Operational Management	3.8846	.9089	26
Security Management	2.0000	.0000	2
Other	4.1622	.8665	37
Total Cases = 290			
Missing Cases = 48 or 16.6 PCT.			

TABLE LIV (Continued)

	Mean	Std Dev	Cases
	CIS-12		
	3.9106	.9857	246
Data Processing Management	3.9171	1.0049	181
Operational Management	3.6154	.8038	26
Security Management	3.0000	1.4142	2
Other	4.1351	.9476	37
Total Cases = 290			
Missing Cases = 44 or 15.2 PCT.			
	CIS-15		
	3.8340	.9504	247
Data Processing Management	3.7956	.9984	181
Operational Management	3.8462	.7845	26
Security Management	3.5000	.7071	2
Other	4.0263	.8216	38
Total Cases = 290			
Missing Cases = 43 or 14.8 PCT.			

TABLE LV

BREAKDOWN OF TOP FIVE COURSES COMPARED TO RESPONDENT'S PRESENT POSITION

	CIS-13	CIS-6	CIS-7	CIS-12	CIS-15
Data Processing Management	4.807	4.0331	3.9266	3.9171	3.7956
Operational Management	4.3077	3.9615	3.8846	3.6154	3.8462
Security Management	3.0000	2.5000	2.0000	3.0000	3.5000
Other	4.7027	4.0526	4.1622	4.1351	4.0263

TABLE LVI

RESPONDENT'S TIME IN PRESENT POSITION COMPARED
TO INDIVIDUAL TOP FIVE COURSES

	Mean	Std Dev	Cases
	CIS-13		
	4.4837	.8462	246
Less 1 year	4.2727	1.1531	33
1 - 2 years	4.6364	.8594	33
3 - 4 years	4.5584	.6976	77
5 - 6 years	4.5250	.5986	40
Over 6 years	4.3871	.9470	62
Total Cases = 290			
Missing Cases = 44 or 15.2 PCT.			
	CIS-6		
	4.0162	.9150	247
Less 1 year	4.1212	1.0234	33
1 - 2 years	4.0000	1.0150	34
3 - 4 years	4.0519	.8094	77
5 - 6 years	3.8750	.9111	40
Over 6 years	4.0161	.9494	62
Total Cases = 290			
Missing Cases = 43 or 14.8 PCT.			
	CIS-7		
	3.9421	.9921	242
Less 1 year	3.8485	.9722	33
1 - 2 years	3.7941	1.1489	34
3 - 4 years	4.1842	.8440	76
5 - 6 years	3.8462	1.0647	39
Over 6 years	3.8644	.9906	59
Total Cases = 290			
Missing Cases = 48 or 16.6 PCT.			

TABLE LVI (Continued)

	Mean	Std Dev	Cases
	CIS-12		
	3.9106	.9857	246
Less 1 year	3.9697	.9515	33
1 - 2 years	3.7273	1.1798	33
3 - 4 years	3.9740	.9594	76
5 - 6 years	3.7750	.9195	40
Over 6 years	4.0000	.9983	62
Total Cases = 290			
Missing Cases = 44 or 15.2 PCT.			
	CIS-15		
	3.8340	.9504	247
Less 1 year	3.7273	1.0390	33
1 - 2 years	3.9118	.9651	34
3 - 4 years	3.8571	.8990	77
5 - 6 years	3.9750	.8317	40
Over 6 years	3.7258	1.0428	62
Total Cases = 290			
Missing Cases = 43 or 14.8 PCT.			

TABLE LVII

BREAKDOWN OF RESPONDENT'S TIME IN PRESENT POSITION COMPARED TO INDIVIDUAL TOP FIVE COURSES

	CIS-13	CIS-6	CIS-7	CIS-12	CIS-15
Less than 1 year	4.2727	4.1212	3.8485	3.9697	3.7273
1 - 2 years	4.6364	4.0000	3.7941	3.7273	3.9118
3 - 4 years	4.5584	4.0519	4.1842	3.9740	3.8571
5 - 6 years	4.5250	3.8750	3.8462	3.7750	3.9750
Over 6 years	4.3871	4.0161	3.8644	3.9839	3.7258
Other	5.0000	4.0000	2.0000	4.0000	4.0000

TABLE LVIII

RESPONDENT'S COMPUTER-RELATED EXPERIENCE
COMPARED TO TOP FIVE COURSES

	Mean	Std Dev	Cases
	CIS-13		
	4.4877	.8437	244
Less 1 year	5.0000	.0000	1
1 - 2 years	3.0000	1.4142	2
3 - 4 years	4.8571	.3780	7
5 - 6 years	4.7692	.4385	13
7 - 10 years	4.4857	.9813	35
Over 10 years	4.4677	.8328	186
Total Cases = 290			
Missing Cases = 46 or 15.9 PCT.			
	CIS-6		
	4.0122	.9165	245
Less 1 year	3.0000	.0000	1
1 - 2 years	3.0000	2.8284	2
3 - 4 years	4.1429	.8997	7
5 - 6 years	4.3846	.6504	13
7 - 10 years	4.0000	.9701	35
Over 10 years	4.0000	.8990	187
Total Cases = 290			
Missing Cases = 45 or 15.5 PCT.			
	CIS-7		
	3.9500	.9882	240
Less 1 year	2.0000	.0000	1
1 - 2 years	3.0000	2.8284	2
3 - 4 years	4.4286	.5345	7
5 - 6 years	4.3846	.5064	13
7 - 10 years	3.9412	.9829	34
Over 10 years	3.9235	.9915	183
Total Cases = 290			
Missing Cases = 50 or 17.2 PCT.			

TABLE LVIII (Continued)

	Mean	Std Dev	Cases
	CIS-12		
	3.8327	.9542	245
Less 1 year	5.0000	.0000	1
1 - 2 years	3.5000	.7071	2
3 - 4 years	4.2857	.7559	7
5 - 6 years	3.8462	.7470	13
7 - 10 years	3.9714	.9871	35
Over 10 years	3.7861	.9931	187
Total Cases = 290			
Missing Cases = 45 or 15.5 PCT.			
	CIS-15		
	3.9139	.9880	244
Less 1 year	2.0000	.0000	1
1 - 2 years	1.5000	.7071	2
3 - 4 years	4.2857	1.1127	7
5 - 6 years	4.0769	.8623	13
7 - 10 years	3.8286	.9848	35
Over 10 years	3.9409	.9596	186
Total Cases = 290			
Missing Cases = 46 or 15.9 PCT.			

TABLE LIX

BREAKDOWN OF RESPONDENT'S COMPUTER-RELATED EXPERIENCE
COMPARED TO TOP FIVE COURSES

	CIS-13	CIS-6	CIS-7	CIS-12	CIS-15
Less than 1 year	5.0000	3.0000	2.0000	5.0000	2.0000
1 - 2 years	3.0000	3.0000	3.0000	3.5000	1.5000
3 - 4 years	4.8571	4.1429	4.4286	4.2857	4.2857
5 - 6 years	4.7692	4.3846	4.3846	3.8462	4.0769
7 - 10 years	4.4857	4.0000	3.9412	3.9714	3.8286
Over 10 years	4.4677	4.0000	3.9235	3.7861	3.9409

TABLE LX

RESPONDENT'S HIGHEST EDUCATIONAL LEVEL
COMPARED TO TOP FIVE COURSES

Topic	Mean	Std Dev	Cases
	CIS - 13		
	4.4836	.8485	244
High School Grad	4.3333	.5000	9
Some College	4.2642	1.0029	53
Associate Degree	4.4444	.8006	27
Vocational/Technical	4.6667	.4924	12
Bachelor's Degree	4.5300	.8814	100
Master's Degree	4.6429	.6922	42
Doctoral Degree	5.0000	.0000	1
Total Cases = 290			
Missing Cases = 46 or 15.9 PCT.			
	CIS - 6		
	4.0204	.9164	245
High School Grad	3.8889	.7817	9
Some College	3.9245	1.0349	53
Associate Degree	4.0370	.9398	27
Vocational/Technical	4.1667	.7177	12
Bachelor's Degree	4.1782	.8049	101
Master's Degree	3.7143	1.0109	42
Doctoral Degree	5.0000	.0000	1
Total Cases = 290			
Missing Cases = 45 or 15.5 PCT.			
	CIS - 7		
	3.9502	.9862	241
High School Grad	4.1111	.7817	9
Some College	3.7843	1.0259	51
Associate Degree	4.1111	1.0127	27
Vocational/Technical	4.0833	.6686	12
Bachelor's Degree	4.0400	.9941	100
Master's Degree	3.7317	1.0006	41
Doctoral Degree	5.0000	.0000	1
Total Cases = 290			
Missing Cases = 49 or 16.9 PCT.			

TABLE LX (Continued)

Topic	Mean	Std Dev	Cases
	CIS - 12		
	3.9180	.9821	244
High School Grad	4.1111	.6009	9
Some College	3.8113	1.0201	53
Associate Degree	3.7778	.8916	27
Vocational/Technical	3.6667	.6513	12
Bachelor's Degree	4.0100	1.0492	100
Master's Degree	3.9524	.9866	42
Doctoral Degree	4.0000	.0000	1
Total Cases = 290			
Missing Cases = 46 or 15.9 PCT.			
	CIS - 15		
	3.8268	.9513	245
High School Grad	3.7778	.6667	9
Some College	3.6415	.9824	53
Associate Degree	3.7407	.9027	27
Vocational/Technical	4.2500	.8660	12
Bachelor's Degree	3.8515	.9735	101
Master's Degree	3.9286	.9472	42
Doctoral Degree	5.0000	.0000	1
Total Cases = 290			
Missing Cases = 45 or 15.5 PCT.			

TABLE LXI

BREAKDOWN OF RESPONDENT'S HIGHEST EDUCATIONAL LEVEL COMPARED TO TOP FIVE COURSES

	CIS-13	CIS-6	CIS-7	CIS-12	CIS-15
High School Graduate	4.3333	3.8889	4.1111	4.1111	3.7778
Some College	4.2642	3.9245	3.7843	3.8113	3.6415
Associate Degree	4.4444	4.0370	4.1111	3.7778	3.7407
Vocational/ Trade School Certificate	4.6667	4.1667	4.0833	3.6667	4.2500
Bachelor's Degree	4.5300	4.1782	4.0400	4.0100	2.8515
Master's Degree	4.6429	3.7143	3.7317	3.9524	3.9286
Doctoral Degree	5.0000	5.0000	5.0000	4.0000	5.0000

graduate category. CIS-15's highest category was in the vocational/ technical school category. The only respondent in the doctoral degree category tended to rate all courses as a five, except CIS-12.

Section V - Chi-square Test For Significance

Statistics for two-way tables were utilized in comparing various items in the questionnaire. The Chi-square test for significance was computed for each of the comparisons. The .05 level of significance was selected for this study. The following information for each cell in the two-way tables is given: observed frequency, row percent, column percent. Column and row totals and percentages are also given along with the results of the Chi-square test and the significance level.

Selected independent variables were compared to two dependent variables:

1. Section III-1 of the questionnaire which seeks the respondent's "yes" or "no" response to whether they feel computer center employees should possess some knowledge about computer security.
2. Section IV-2 of questionnaire which asks the respondent to indicate which of the following methods would best develop computer security knowledge:
    a. Complete course in computer security in addition to incorporation of computer security topics in the Computer Information Systems Curriculum.
    b. Complete course in computer security ONLY.
    c. Incorporation of computer security topics into the current courses in the computer Information Systems (CIS) Curriculum ONLY.

d. Other method.

The independent variables are:

1. Section I-2 of questionnaire. Number of people presently employed in respondent's computer center.
2. Section I-3. Whether respondent's computer center has a designated person responsible for computer security.
3. Section I-4. Number of people in respondent's organization who are DIRECTLY responsible for computer security as stated in their job description.
4. Section II-1 of questionnaire. Respondent's present position.
5. Section II-2 of questionnaire. Length of time respondent has been in their present position.
6. Section II-3 of questionnaire. Length of time respondent has been employed in a computer-related position.
7. Section II-4 of questionnaire. Highest education level of respondent.
8. Section II-4 of questionnaire. Major area of study of respondent.
9. Section II-5 of questionnaire. Educational or training areas utilized by the respondent in computer security.
10. Section II-6. Number of employees presently supervised by respondent at the present time.
11. Section II-7. Respondent's membership(s) in data processing professional organizations.

After comparing the dependent variables individually to each of the eleven independent variables, the two dependent variables were compared to each other to test for significance.

The Chi-square tests showing a significant difference will be included in the discussion here in Chapter IV. All Chi-square tests showing no significant difference will be shown in Appendix J.

Comparison of Whether Respondent Feels Computer Center Employees Should Possess Same Knowledge About Computer Security to Specific Questionnaire Sections

Number of Employees in Respondent's Computer Center. Table LXXVIII in Appendix J shows that there was no significant difference between whether respondent feels computer center employees should possess some knowledge and number of employees in respondent's computer center.

Whether Respondent's Computer Center Had a Designated Person Directly Responsible for Computer Center. Table LXXIX in Appendix J shows that there was no significant difference between whether respondent feels computer center employees should possess some knowledge and whether the respondent's computer center had a designated person responsible for computer security.

Number of Persons in Respondent's Computer Center Directly Responsible for Computer Security. Table LXXX in Appendix J shows that there was no significant difference between whether respondent feels computer center employees should possess some knowledge and whether the number of persons in the respondent's computer center who are directly responsible for computer security as stated in their job description.

Respondent's Present Position. Table LXXXI in Appendix J shows that there was no significant difference between whether respondent feels computer center employees should possess some knowledge and the respondent's present position.

Respondent's Length of Time in Present Position. Table LXXXII in Appendix J shows that there was no significant difference between whether respondent feels computer center employees should possess some knowledge and the respondent's length of time in present position.

Respondent's Length of Time in a Computer-Related Position. Table LXII shows that there is a significant difference at the .05 level between whether respondent feels computer center employees should possess some knowledge and the respondent's length of time in a computer-relatd position. The "yes" responses in the 3 -4 year category were 2.1 percent compared to 1.7 percent in the "no" category. The "yes" responses in the 5 - 6 year category were 4.5 percent compared to .7 percent in the "no" category. The "yes" responses in the 7 - 10 year category were 12.2 percent compared to 2.1 percent in the "no" category. In the over 10 year category, the "yes" responses were 65.6 percent and the "no" category were 9.0 percent. It would appear that the longer a person is employed in a computer related position, the more concerned they become about computer security.

This difference may be attributed to the fact that the respondents are in the data processing or operational management job function category and, therefore, tend to be at the uppper echelons of the computer center organization. Most of these positions will tend to be occupied by persons who have accumulated knowledge or expertise over a number of years, rather than merely completing a course of study in the computer area.

Respondent's Highest Educational Level. Table LXXXIII in Appendix J shows that there was no significant difference between whether the respondent feels computer center employees should possess some knowledge and the respondent's highest educational level.

TABLE LXII

COMPARISON OF WHETHER COMPUTER CENTER EMPLOYEES SHOULD POSSESS KNOWLEDGE OF COMPUTER SECURITY AND RESPONDENT'S LENGTH OF TIME IN A COMPUTER-RELATED POSITION

Knowl-edge	Less 1 Year	1-2 Years	3-4 Years	5-6 Years	7-10 Years	Over 10 Years	Row Total
Yes	1	2	6	13	35	189	246
	.4	.8	2.4	5.3	14.2	76.8	85.4
	50.0	50.0	54.5	86.7	85.4	87.9	
	.3	.7	2.1	4.5	12.2	65.6	
No	1	2	5	2	6	26	42
	2.4	4.8	11.9	4.8	14.3	61.9	14.6
	50.0	50.0	45.5	13.3	14.6	12.1	
	.3	.7	1.7	.7	2.1	9.0	
Column Total	2	4	11	15	41	215	288
	.7	1.4	3.8	5.2	14.2	74.7	100.0

X^2 = 15.54701 (D.F. = 5) P < .01 < .05

Significance = 0.0083

Respondent's Major Area of Study. Table LXXXIV in Appendix J shows that there is no significant difference between whether the respondent feels computer center employees should possess some knowledge and the respondent's major area of study.

Respondent's Educational or Training in Computer Security. Table LXIII shows that there was a significance at the .05 level between whether the respondent feels computer center employees should possess some knowledge and whether the respondent has utilized some type of education or training areas in computer security. Of the "yes" respondents, 7.6 percent had utilized regular college courses or college extension courses, compared to only 1.0 percent of the "no" respondents. The "yes" respondents utilizing in-house training programs presented by a member of their organization shows 13.5 percent, compared to 1.4 percent of the "no" respondents. The "yes" respondents indicating they utilized seminars offered by other private companies and presented by a member of the respondent's organization's staff, including vendor-sponsored seminars was 23.9 percent, compared to 2.1 percent of the "no" respondents. The respondent's who indicated that they utilized self-education (i.e. independent reading and study) was 27.0 for "yes" and 4.5 for "no". Those indicating no training/education in data security were 13.5 percent for the "yes" responses and 5.5 percent for the "no" responses. These figures would seem to indicate that those respondents who have utilized some method of education/training in computer security also feel that computer center employees should possess some knowledge of computer security (85.5 percent for "yes" compared to 14.5 percent for "no").

Number of Employees Directly Supervised by Respondent. Table LXXXV in Appendix J shows that there was no significant difference between

TABLE LXIII

COMPARISON OF WHETHER COMPUTER CENTER EMPLOYEES SHOULD POSSESS KNOWLEDGE OF COMPUTER SECURITY AND RESPONDENT'S EDUCATION/TRAINING IN COMPUTER SECURITY

Know-ledge	College Courses	In-House Train	Seminars	Self-Education	No Training	Row Total
Yes	22	39	69	78	39	247
	8.9	15.8	27.9	31.6	15.8	85.5
	88.0	90.7	92.0	85.7	70.9	
	7.6	13.5	23.9	27.0	13.5	
No	3	4	6	13	16	42
	7.1	9.5	14.3	31.0	38.1	14.5
	12.0	9.3	8.0	14.3	29.1	
	1.0	1.4	2.1	4.5	5.5	
Column Total	25	43	75	91	55	289
	8.7	14.9	26.0	31.5	19.0	100.0

X^2 = 13.04240 (DF = 4) P < . 05

Significance = 0.0111

whether the respondent feels computer center employees should possess some knowledge and respondent's membership in data processing professional organizations.

Table LXXXVI in Appendix J shows that there was no significant difference between whether the respondent feels computer center employees should possess some knowledge and respondent's membership in data processing professional organizations.

Section VI - Additional Comments Supplied by Respondent

The respondents were provided space at the end of the questionnaire to include any additional comments and suggestions relating to the questionnaire, the study being conducted, or the subject of computer security. The respondents were very liberal with their comments and to insure completeness of this study, selected comments are included in this section.

<u>Relating to the Questionnaire</u>.

"Should address in-house security along with service bureau security. In-house has a lot to learn from the service industry."

"Legal aspects of computer security should be given more emphasis."

<u>Relating to the Study Being Conducted</u>.

"I think it's a good idea to incorporate the degree of security related to a specific course."

"Topics of security, operations, backups, etc., are better learned on the jobs. These topics should be addressed in introductory classes, however."

"A section on developing a step-by-step disaster recovery plan is recommended for a computer security course."

"I would suggest a risk analysis course that would teach methods of evaluating risks and solutions financially."

"Security should be a part of all data processing courses."

Relating to the Subject of Computer Security.

"Would prefer training in security systems remain outside of normal college curriculums; security is best based on ignorance or incomplete understanding."

"There is a need to foster concern and respect for maintaining the integrity of hardware/software and the corporate/institutional data they control."

"The goals of data security and privacy may not always be the same or of equal emphasis."

"Information systems probably have better security (even the worst) than most manual systems at their best."

"The strength of emphasis in certain security areas will differ considerably based on the nature of the business."

"Good computer security has to be built in, not added on."

"As caretakers of a company's most vital assets and data, computer professionals must view the operation from all perspectives. What is not seen from one vantage point will be observed from another."

"Computer security encompasses bother the physical and intellectual aspects of the institution."

Comparison of Methods Respondents Feel Would Best Develop Computer Security Knowledge to Specific Questionnaire Sections

Number of Employees in Respondent's Computer Center. Table LXXXVII in Appendix J shows that there was no significant difference between the methods the respondents feel would best develop computer security knowledge and the number of employees in the respondent's computer center.

Whether Respondent's Computer Center has a Designated Person Directly Responsible For Computer Security. Table LXXXVIII in Appendix J shows that there was no significant difference between the methods the respondents feel would best develop computer security knowledge and whether the respondent's computer center had a designated person responsible for computer security.

Number of Persons in Respondent's Computer Center Directly Responsible For Computer Security. Table LXXXIX in Appendix J shows that there was no significant difference between the methods the respondents feel would best develop computer security knowledge and the number of persons in respondent's computer center directly responsible for computer security.

Respondent's Present Position. Table LXXXX in Appendix J shows that there was no significant difference between the methods the respondents feel would best develop computer security knowledge and the respondent's present position.

Respondent's Length of Time in Present Position. Table LXXXXI in

Appendix J shows that there was no significant difference between the methods the respondents feel would best develop computer security knowledge and the respondent's length of time in their present position.

Respondent's Length of Time in Computer-Related Position. Table LXXXXII in Appendix J shows that there was no significance between the methods the respondents feel would best develop computer security knowledge, and the respondent's length of time in a computer-relation position. It is interesting to note, however, that the level of significance, .0911, while not significant at the .05 level, there does seem to be a tendency for experience level to be related to this dependent variable. When comparing the computer-related experience to the first dependent variable, a significance level was shown.

Respondent's Highest Educational Level. Table LXXXXIII in Appendix J shows that there was no significant difference between the methods the respondents feel would best develop computer security knowledge and the respondent's highest educational level.

Respondent's Major Area of Study. Table LXXXXIV in Appendix J shows that there was no significant difference between the methods the respondents feel would best develop computer security knowledge and the respondent's major area of study.

Respondent's Education or Training in Computer Security. Table LXXXXV in Appendix J shows that there was no significant difference between the methods the respondents feel would best develop computer security knowledge and the respondent's education or training in computer security.

Number of Employees Directly Supervised by the Respondent. Table LXXXXVI in Appendix J shows that there was no significant difference between the methods the respondents feel would best develop computer security knowledge and the number of employees directly supervised by the respondent.

Respondent's Membership in Data Processing Professional Organizations. Table LXXXXVII in Appendix J shows that there was no significant difference between the methods the respondents feel would best develop computer security knowledge and the respondent's membership in data processing professional organization.

Comparing Two Dependent Variables. Table LXXXXVIII in Appendix J shows that there was no significant difference between whether the respondent feels computer center employees should possess some knowledge about computer security and the methods the respondent feels would best develop computer security knowledge.

Summary

This chapter presented a detailed analysis of the results gathered from the study instrument. The analysis of the data obtained from the study instrument was divided into six sections:

1. Frequency distributions that analyzed the use of electronic data processing by the respondent's firm, an analysis of the personal information about the respondent, and the analysis of the business information about the respondent.
2. Rankings by means of computer security topics.
3. Rankings by means of courses, both core and elective, from the DPMA Model Curriculum.

4. Cross tabulations of Sections 2 and 3 above where comparisons are made between demographic data (Sections I and II of questionnaire) and selected security topics and core and elective courses.
5. Chi-squares on Section IV to test for significance.
6. An Interpretative Summary of the respondents' narrative comments.

The results of each item were tabulated and presented according to the frequency of occurence, accumulative frequency, percentage, and accumulative percentage. Two-way tables and the Chi-square test for significance were utilized in comparing and revealing relationships between selected items appearing in the study instrument. Specific results were summarized and reported through detailed discussions and tables shown with this chapter and Appendices G, H, I, and J.

The summary, conclusions, and recommendations are presented in Chapter V.

CHAPTER V

SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS

The past decade has seen the rapid development and proliferation of computers in organizations of all sizes and types. Often, as this growth proceeded, security was not considered in the system design stages. Except where security has been very obviously of major importance (e.g., in banking systems or top secret military or defense research projects) it has often been conveniently ignored by designers of computer systems.

The problem of data security becomes even more paramount and complex as our present office environment becomes increasingly automated. Managers will have to be versatile and innovative in "juggling" the demands of technology, information, and people. The threats to security become even more paramount as systems increase in complexity.

In order for office personnel to be prepared for such roles, colleges and universities must begin to recognize the urgent need to enhance their curricula by including data security topics so that college graduates entering the business environment are cognizant of the importance of data security. In order to keep our curricula as current as possible, we must constantly assess whether or not we are meeting the needs of business and industry.

Purpose and Design of the Study

The purpose of this study was to provide information indicating whether computer center personnel feel college students in Computer

Information Systems (CIS) programs should become more aware of the importance of computer security. This was accomplished by an interpretative analysis of data obtained from questionnaires mailed to DPMA members on the operational or data processing management level throughout the United States.

The Questionnaire

To help achieve the purposes of this study, a six-page questionnaire was designed. The questionnaire was developed from a study of the literature, review of numerous other questionnaires, and consultations with various faculty members at Oklahoma State University. The questionnaire was mailed to 700 DPMA members throughout the United States in the Spring of 1984. A total of 299 or 43.8 percent, of the members contacted responded to the questionnaire.

Analysis of the Data

All the responses to the questionnaire were coded and analyzed using the SPSS-X statistical software package. Frequency counts and percentage relationships were utilized to analyze the descriptive data. Two-way tables and Chi-square tests for significance were used to analyze the comparison of selected items in the questionnaire.

Review of Related Literature

This study was designed to address the issue of computer security by analyzing the opinions of Data Processing Management Association members concerning inclusion of security-related topics into the Computer Information Systems (CIS) curriculum. In order to assess these opinions fully, a thorough review of related literature was conducted to address fully the two main emphasis areas:

1. Review of computer security.
2. Curricular concerns relating to computer security.

Many articles have been written about computer security or curricular concerns in the CIS program, but there is little evidence of tieing the two topics together.

This study further extends knowledge of information systems education by reporting in detail the opinions of DPMA members concerning the topic of incorporating computer security into an existing CIS program.

Results of the Study

The results of the study are summarized in five sections according to:

1. An analysis of the use of electronic data processing by the respondent's firms, an analysis of the respondent's personal information, and an analysis of the business information about respondent.
2. Rankings indicating the importance of selected computer security topics.
3. Rankings indicating the importance of incorporating computer security into selected CIS courses.
4. Comparisons of Topics and Courses to selected parts of the questionnaire.
5. Chi-square tests for significance on selected items in the questionnaire.

Analysis of the Use of EDP by the Respondent's Firm, Analysis of Respondent's Personal and Business Information

IBM tended to dominate the utilization of computer equipment being used in the respondent's computer center, with 45.9 percent, with IBM Model 4341 representing the largest share of the IBM model line, or 31.8 percent.

Fifty-nine percent of the respondent reported that their computer centers had 1 - 20 employees.

The number of respondents who reported that their computer center had a designated person responsible for computer security was 48.6 percent. The remaining 51.4 percent responded that they had no such person.

Of the 48.6 percent of the respondents who reported that their computer center did not have a designated person responsible for computer security, 22.1 percent had one person, 16.6 percent had two persons, and only 1.0 percent had seven or more persons.

The title of person(s) directly responsible for computer security was listed as Operations Manager/Supervisor/Director in 40.4 percent of the responses and 17.1 percent in the Data Processing or Information Systems Director/Manager category. "Other" titles were listed in 19.2 percent of the responses.

Of the respondents who indicated that their computer center did <u>not</u> have a designated person responsible for computer security, 35.9 percent indicated that computer security is performed as part of other responsibilities and NOT listed as a separate job function.

Of the respondents, 19.7 percent indicated that their organization had <u>no formal</u> program in computer security, and 42.8 percent utilized other methods of computer security analysis.

Almost three-fourths, or 73.4 percent, of the respondents were in the data processing management category, and 10.0 percent were in the operational management category.

Nearly one-third, or 30.7 percent, of the respondents have been in their present position from three to four years, over one-fourth, or 26.6 percent, have been in their present position for more than six years. These figures indicate also that only 12.8 percent had been in their present position for less than one year.

Nearly three-fourths of the respondents have been in a computer-related position for more than ten years. Only 0.7 percent, or two respondents, had been in a computer-related position for less than one year.

The highest educational level of the respondents showed that 22.1 percent (nearly one-fourth) had some college work, but had not earned a degree. Eleven percent held an associate degree. Over one-third, 38.6 percent, were awarded a Bachelor's Degree, and 16.9 percent held Master's Degrees.

Almost one-third, 32.1 percent, held business degrees, and nearly one-fourth, 23.1 percent, held a degree in computer science or data processing.

In order to gain knowledge in computer security, 42.9 percent of the respondents utilized self-education, 25.9 percent indicated that they attended seminars, 12.3 percent attended in-house seminars, 5.7 percent attended regular college or college extension courses, and 13.2 percent indicated that they had no training or education in data security.

Over one-third, 29.0 percent, of the respondents reported that they directly supervised from one to five employees at the present time.

One-fifth, 19.0 percent, supervised from 6 to 10 employees, 12.1 percent supervised from 11 to 15 employees. Over 10 percent, 11.7 percent, directly supervised more than 25 employees.

Over three-fourths of the respondents, 77.9 percent, currently hold memberships in DPMA.

Over half, 50.3 percent, of the 290 respondents indicated that they were familiar with the DPMA Model Curriculum.

More than four-fifths, 85.5 percent, felt that computer center employees should possess some knowledge about computer security.

Of the 14.5 percent who indicated that computer center employees do not need to possess computer security knowledge, over half, 53.5 percent, indicated that computer security should be handled only by those who are directly involved in administering security programs. More than two-fifths, or 43.7 percent, indicated that it is not necessary for most employees to possess security information in order to efficiently perform their jobs.

When questioning the respondents concerning the best methods to develop computer security knowledge, over one-third, 39.0 percent, felt that a complete course in computer security in addition to incorporation of computer security topics in the CIS curriculum would best accomplish this desired knowledge. Those favoring incorporation ONLY represented 37.2 percent. Only 6.9 percent indicated that a complete course ONLY would be best.

Rankings of Selected Computer Security Topics by Means

When asked to rank the importance of selected topic areas that might be considered for inclusion in the Computer Information Systems

Curriculum relating to the topic of computer security, the top five topics were: Overview of Computer Security, Disaster Protection, EDP Controls and Audit, Software Protection, and Fire Protection. All five topics had a mean of over 4.0 on a 1 - 5 scale, where 5 represented Very Important.

Rankings of Inclusion of Computer Security Into Selected Courses in the CIS Curriculum

When asked to rank the importance of including elements of computer security into selected courses in the DPMA Model Curriculum, the top five courses, ranked by means, were CIS-13, EDP Audit and Controls; CIS-6, Database Program Development; CIS-7, Applied Software Development Project; CIS-12, Distributed Data Processing; and CIS-15, Information Resource Management.

Comparisons of Topics and Courses to Selected Parts of the Questionnaire

The top five topics and top five courses were then compared to selected items in the questionnaire to indicate a thorough breakdown of opinions of the DPMA respondents in each of these topics and courses. A detailed listing of this breakdown is given in Chapter IV. The breakdowns for topics and courses other than the top five are shown in Appendices G, H, and I.

Chi-square Tests for Significance

Selected independent variables were compared to two dependent variables:

1. The respondent's "yes" or "no" response as to whether they feel computer center employees should possess some knowledge about computer security.
2. Methods respondents feel would best develop computer security knowledge.

There was a significant difference at the .05 level between whether the respondent feels computer center employees should possess some computer security knowledge and the respondent's length of time in a computer-related position. The "yes" responses in the 3 - 4 years category were 2.1 percent compared to 1.7 percent in the "no" category. The "yes" responses in the 5 - 6 years category were 4.5 percent compared to .7 percent in the "no" category. The "yes" responses in the 7 - 10 years category were 12.2 percent compared to 2.1 percent in the "no" category. In the over 10 years category, the "yes" responses were 65.6 percent and the "no" responses were 9.0 percent. It would appear that the longer persons are employed in computer-related positions, the more concerned they become about computer security.

There was a significant difference at the .05 level between whether the respondent feels computer center employees should possess some knowledge about computer security and whether the respondents have utilized some type of education or training areas in computer security. Of the "yes" respondents, 7.6 percent had utilized regular college courses or college extension courses, compared to only 1.0 percent of the "no" respondents. The "yes" respondents utilized in-house training programs presented by a member of their organization in 13.5 percent of the responses, compared to 1.4 percent of the "no" respondents. The "yes" respondents indicated they utilized seminars offered by other private companies and presented by a member of the respondent's organization's staff, including vendor-sponsored seminars, was 23.9 percent, compared to 2.1 percent of the "no" respondents. The respondents who indicated that they utilized self-education (i.e., independent reading and study) was 27.0 percent for "yes" and 4.5 for "no". Those indicating no training/education in data security were 13.5 percent for "yes" responses and 5.5 percent for "no" responses. These figures would seem to indicate that those respondents who have utilized some method of education/training in computer security also feel that computer center employees should possess some knowledge of computer security (85.8 percent for those who responded "yes" compared to 14.5 percent for those who responded "no").

Conclusions and Recommendations

The following conclusions and recommendations are based on the results of the descriptive analysis of responses by DPMA members in the data processing or operational management category and on the review of related literature.

1. The review of related literature indicated that managers in the future will have to be versatile and innovative in meeting the demands of technology, information, and people. As these threats to computer security become more numerous, managers may need a larger base of knowledge in order to perform their jobs effectively.

2. The review of related literature indicated that sources of threats to computer security encompass virtually all areas in the computer environment. Measures should be instituted to ensure that all areas are sufficiently covered in order to insure an efficient on-going security program.

3. The review of related literature indicated that students in university and college business and computer courses are presently offered very little in terms of computer security awareness.

4. The review of related literature indicated that programs must be designed to give the student a broad-based background with a high emphasis on new technological equipment found in the business office.

5. The review of related literature repeatedly verified the extent of computer abuse but also indicates that there are no accurate estimates of the total losses to business and to the government each year through computer crimes as many companies and agencies are reluctant to admit vulnerability. Estimates of reported breaches range from 10 to 20 percent of the total number of violations occurring each year.

6. The review of the related literature indicated the fact that today's organizations are dependent upon data processing services, creating a unique vulnerability for many organizations never before experienced in the business environment.

7. The review of related literature indicated that computer security training and awareness encompasses two groups: those who implement, maintain, and operate the system; and those who use the system.

8. The review of the related literature indicated that the DPMA Model Curriculum does suggest more than a superficial view of the security problem, particularly in the EDP Audit course.

9. One of the pilot study respondents indicated that computer security should be taught as an attitude rather than as a technology as most businesses have common attitudes toward data security but the technology can vary between companies and vendors.

10. Additional comments provided by some of the respondents

indicated that the knowledge of computer security can best be attained on-the-job, not in a college classroom. One respondent felt that the most effective way to gain knowledge was to experience a disaster.

11. Other respondents, conversely, indicated in their additional comments that computer security should be included in all computer or data processing education.

12. The presence of "small shops" of 1 to 20 employees represented over half of the computer centers in this study.

13. Less than half of the respondents surveyed had a designated person directly responsible for computer security, with most reporting only one or two persons responsible according to their stated job descriptions. Over one-third indicated that computer security was performed as part of other duties and not listed as a separate job function. This would seem to indicate that many computer centers are not fully addressing the issue of computer security to meet current demands.

14. There is a tendency for persons to view computer security as more of an important issue when they have been employed in computer-related positions for longer periods of time.

15. Almost half of the respondents gained computer security knowledge through self-education, rather than through formal education channels.

16. There is a tendency for those utilizing some type of training or education in computer security to feel that computer center employees should possess some knowledge about computer security.

17. Only half of the respondents were familiar with an information systems model curriculum, thus indicating that more interaction between computer professionals and educators may be necessary in order to

develop the knowledges needed by computer center employees.

18. A large majority of respondents, over 80 percent, indicated that computer center employees should possess some knowledge about computer security.

19. To best accomplish this computer security knowledge base in the CIS curriculum, two methods were preferred by the respondents: a complete course in computer security in addition to incorporation of computer security topics in the CIS curriculum; and incorporation into the existing curriculum only.

20. The top five topics chosen by the respondents to be included in the Computer Information Systems Curriculum relating to the topic of computer security were: Overview of Computer Security, Disaster Protection, EDP Controls and Audit, Software Protection, and Fire Protection.

21. Computer security should be included in the following CIS courses: EDP Audit and Controls, Database Program Development, Applied Software Development Project, Distributed Data Processing, and Information Resource Management.

22. Based on these findings, the researcher recommends that the CIS curriculum should be constantly assessed and evaluated by both educators and practitioners in order to coordinate desired data processing and computer knowledge levels.

Recommendations for Future Research

1. Similar studies should be conducted to obtain information concerning the opinions of educators concerning inclusion of computer security in the CIS curriculum. Groups to be considered might be

educators in the colleges of business, educators in CIS programs, or educators in Computer Science Programs.

2. Data processing professionals should be surveyed to obtain information on the changing technology and the effects those changes have on computer security curriculum.

3. Similar studies could be conducted to obtain information concerning the opinions of management-level employees, outside the computer center, concerning inclusion of computer security topics in the CIS curriculum.

4. Opinions should be sought from computer security practitioners concerning their opinions that the inclusion of computer security topics in the CIS curriculum. The Computer Security Institute would be a suggested group to be utilized for this particular study.

5. Information concerning the opinions of data processing professionals about computer security, should be obtained, utilizing a less select group, such as a DPMA general membership listing.

6. Similar studies should be conducted to obtain information concerning the opinions of data processing professionals concerning computer security, utilizing selected industries, such as banking, governmental agencies, attorneys, public service agencies, manufacturing, in order to ascertain whether the type of operation influences the opinions of the respondents.

7. Studies to obtain information concerning the inclusion of computer security into other model curricula, such as ACM and IEEE should be undertaken.

8. Studies should be conducted to compare one type of group's opinions with another group's opinions, i.e. educators compared to

management, urban compared to rural setting, and "small shops" compared to "large shops".

9. In-depth studies should be conducted seeking the opinions of the respondents concerning the topics to be included. A thorough, inclusive list of topics, along with their complete descriptions, should be utilized for this study in order to prevent overlap and duplication.

10. More studies are needed to determine the computer security knowledge needed by graduates of both CIS programs and College of Business programs.

11. An in-depth study concentrating on the areas of microcomputers, teleprocessing, telecommunications, remote job entry, distributed data processing, and data communications should be conducted to determine the effect of computer security considerations on these rapidly growing technologies.

12. In-depth studies should be conducted in all the suggested course areas in the DPMA Model Curriculum and ACM Model Curriculum to determine the effectiveness and usefulness of these two models.

13. Methodology of teaching CIS courses should be addressed in further research to determine the best methods to instill the knowledge needed by CIS graduates.

14. Studies about all aspects of computer security, and the effect violations have on the general public, should be conducted to keep pace with our increasingly automated environment. Issues to be considered might be legal ramifications of computer security, privacy and confidentiality considerations, and cost effectiveness of security and violations.

REFERENCES CITED

Adams, David R., and Thomas H. Athey, Eds. DPMA Model Curriculum for Undergraduate Computer Information Systems Education. Park Ridge, IL: Data Processing Management Association, September 1981.

Adams, David R., Gerald E. Wagner, and Terrence J. Boyer. Computer Information Systems; An Introduction. Cincinnati: South-Western Publishing Co., 1983.

AFIPS System Review Manual on Security, 1974. Montvale, NJ: American Federation of Information Processing Societies, Inc., February 1975.

Armer, P. "Computer Technology and Surveillance." Computers and People, Vol. 24 (September 1975), pp. 8-11.

Athey, Thomas H. "DPMA's CIS Curriculum '81." Interface, The Computer Education Quarterly, Vol. 3, Issue 3 (Fall 1981), p. 8.

Bartz, Albert E. Basic Statistical Concepts. Minneapolis: Burgess Publishing Company, 1981.

Becker, Hal B. "Network Security in Distributed Data Processing." Data Communication. Vol. 6 (August 1977), pp. 33-39.

Berg, K. L. "Federal Privacy Act Countdown -- Is the Private Sector Ready?" Infosystems, Vol. 22, No. 7 (July 1975), pp. 25-27.

"Beware: Hackers at Play." Newsweek (September 5, 1983), pp. 42-48.

Bloom, Robert. "Computers Don't Commit Crime, People Do." Data Management (July 1983), pp. 14-17.

Bowman, Joel P., and Bernadine P. Branchaw. Business Report Writing. Chicago: The Dryden Press, 1984.

Branstad, M. A., and D. K. Branstad. "Computer Security Applications Utilizing Minis." Proceedings of the 9th Annual IEEE Computer International Conference, COMPCON 74, Fall, Washington, D.C., Paper in Digest of Papers Micros and Minis Application and Design. Washington D.C.: IEEE Computer Society, 1976, pp. 91-94.

Brender, Susan. "Automation for Files Management." Information and Records Management (June 1977), p. 6.

Bund, M. "Security in the Electronic Data Processing Environment." CPA Journal, Vol. 45 (February 1976), pp. 33-35.

Burton, P. A. A Dictionary of Microprogramming. New York: Garland Publishing, Inc., 1976.

Cannon, Francis R. "Skills and Knowledges Required for Data Processing Personnel in Business." The Journal of Data Education, Vol. 18, No. 8 (August 1980), pp. 1-13.

"Computer Crime." Computer Decisions, Vol. 13, No. 6 (June 1981), pp. 104-124.

"Computer Security: A Manager's Guide (Pure and Simple)." Computer Security Institute, 43 Boston Post Road, North Borough, MA 01532, 1983 (see Appendix A).

"Computer Security: What Can Be Done." Business Week (September 26, 1983), pp. 126-130.

Conway, R. W., W. L. Maxwell, and H. L. Morgan. "On the Implementation of Security Measures in Information Systems." Communications of ACM, Vol. 15, No. 4 (April 1972), pp. 211-220.

Cook, James R., Jack D. Eure, Marvin A. Johnston, and Herbert J. Mattord. "DPMA Chapters Speak Out on Data Processing Security." Data Management (May 1982), pp. 42-46.

Cook, James R., Michael C. Gallagher, and Marvin A. Johnsten. "An Analytical Study of Industry's Computer Education Needs." Interface, Vol. 1, No. 1 (Winter 1979), pp. 52-56.

Cotton, I. W. "Network Security." Computer Decisions, Vol. 9 (April 1977), p. 10.

Cotton, I. W., and P. Meissner. "Approaches to Controlling Personal Access to Computer Terminals." Proceedings of 1975 Symposium on Computer Networks: Trends and Application, Gaitherburg, Md., June 18, 1975. Long Beach, CA: IEEE Computer Society, 1975, pp. 32-39.

Couger, J. Daniel, Ed. "Curriculum Recommendations for Undergraduate Programs in Information Systems: A Report of the ACM Curriculum Committee on Computer Education for Management." Communications of the ACM, Vol. 16, No. 12 (December, 1973), pp. 727-749.

Crumley, Marguerite. "A Guide for Advisory Committees in Business Education." Business Education--A Retrospection, Monograph 133. Cincinnati, OH: South-Western Publishing Co., 1978. (Reprinted from The Balance Sheet, April 1948, pp. 1-27.)

Crumpler, John R. "New Curricula Trend Addresses Five DP Job Markets." Data Management (November 1982), pp. 34-35.

Davis, Gordon B. "Information Systems Curricula in the Business School." Interface, Vol. 1, No. 1 (Winter 1979), pp. 2-4.

Davis, R. M. "Implications of Privacy Legislation on the Use of Computer Technology in Business." Jurimetrics Journal, Vol. 17, No 1 (Fall 1976), pp. 95-110.

Davis, R. M. "National Bureau of Standards: Its Role in Computer Security." (Paper presented at the Proceedings IBM Data Security Symposium, Cambridge, MA, April 10-11, 1973, Paper #G-520-28381, pp. 1-11.)

Denning, Dorothy E., and Peter J. Denning. "Certification of Programs for Secure Information Flow." Communications of the ACM, Vol. 20, No. 7 (July 1977), pp. 504-513.

Dennis, J. B. "A Position Paper on Computing and Communications." Communications of ACM, Vol. 11, No. 5 (May 1968), pp. 370-377.

Dershem, Herbert L. "A Survey of Computing in Private Liberal Arts Colleges." The Journal of Data Education, Vol. XIX, No. 2 (January 1979), pp. 7-9.

Dillman, Don A. Mail and Telephone Surveys. New York: John Wiley and Sons, 1978.

Doll, Ronald C. Curriculum Improvement: Decision-Making and Process. Boston, MA: Allyn and Bacon, Inc., 1971.

"DPMA's Model Curriculum Project." Project presented by Data Processing Management Association at DPMA, Philadelphia, October, 1980.

Elmer-Dewitt, Phillip. "The 414 Gang Strikes Again." Time (August 29, 1983), p. 34.

Enger, Norman L., and Paul W. Howerton. Computer Security . . . A Management Audit Approach. New York: Amaco (A Division of American Management Associations), 1980.

Farr, M.A.L., B. Chadwick, and K. K. Wong. Security for Computer Systems. Manchester, England: NCC Publications, 1972.

Fields, Cheryl M. "Colleges Urged to File Lawsuits When Defrauded." The Chronicle of Higher Education, Vol. XXVIII, No. 4 (March 21, 1984), pp. 1 and 12.

Francella, Kevin. "Multiple Controls Combat Computer Crime." Data Management (July 1983), p. 21.

Gaides, R. Stockton, and Norman Z. Shapiro. Some Security Principles and Their Applications to Computer Security--General Concepts of Security, Computer Security. Santa Monica, CA: The Rand Corporation, 1980.

Galloway, Rex F. "Design Innovations for Curriculum in Data Processing and Computer Systems Management." The Journal of Data Education, Vol. XIX, No. 3 (April 1979), pp. 5-7.

Gay, L. R. Educational Research, Competencies for Analysis and Application. Columbus: Charles E. Merrill Publishing Company, 1981.

Goetz, M.A. "Software Protection: You Get Your Company." Infosystems, Vol. 24 (July 1977), p. 60.

Gibbons, John H. Computer-Based National Information Systems . . . . . . Technology and Public Policy Issues. Washington, DC: Office of Technology Assessment, 1981, pp. 1-178.

Golen, Steven, and Herbert Scott. "Identifying Potential Areas of Computer Crime." The Journal of Data Education (Winter 1982-83), pp. 18-19.

Good, Carter V. Essentials of Educational Research, Methodology and Design. New York: Appleton-Century Crafts, 1966.

Guidelines for Establishing a Computer Security Program. Hudson, MA: Computer Security Institute, 1977.

Hamstead, Alan. "A Study of Computer Abuse." (Unpublished paper.) Australia: Caulfield Institute of Technology, February 1979, pp. 1-95.

Heide, Dorothy, and James K. Hightower. "Organizations, Ethics, and the Computing Professional." Journal of Systems Management, Vol. 34, No 11 (November 1983), pp. 38-42.

Hodge, Bartow, Robert Fleck, Jr, and C. Brian Honess. "Producing Realtime Graduates, A 'Live Case' Approach to Information Systems Education." Data Management, Vol. 15, No. 10 (October 1977), pp. 60-63.

Hodge, Bartow, Robert A. Fleck, Jr., and C. Brian Honess. Management Information Systems. Reston, VA: Reston Publishing Co. Inc., 1984.

Hoffberg, Alan. "Protecting Your Computer System Against Unwanted Intrusion Need Not Be Expensive or Difficult." Office Administration and Automation (March 1984), p. 96.

Hoffman, L. J. "Computers and Privacy: A Survey." Computer Survey (January 2, 1969), pp. 85-104.

Hoffman, L. J. Modern Methods for Computer Security and Privacy. Englewood Cliffs, NJ: Prentice Hall, Inc., 1977.

Hollis, G. "Basics of Computer Security." Accountancy, Vol. 88 (January 1977), p. 108.

Howe, Charles L. "Coping With Computer Criminals." Datamation, Vol. 28, No. 1 (January 1982), pp. 118-128.

Hutt, Arthur. "Management's Role in Computer Security." Computer Security Handbook. New York: Macmillan Information, 1972.

Ivarie, Theodore W. "Curricular Concerns About the Changing Office." Business Education Forum (November 1980), p. 17.

Jeffery, S., and D. K. Branstad. "Security Considerations in Software Systems." 3rd Texas Conference on Computing Systems, Austin, Texas, November 7-8, 1974. Long Beach, CA: IEEE Computer Society Publication Office, 1974.

Johnson, Jerry. "Educator's Lexicon of Computerese." Arithmetic Teacher (November 1981), pp. 46-49.

Johnson, Margaret, Ed. "The Changing Office Environment." The National Business Education Yearbook. No. 18. Reston, VA: National Business Education Association, 1980.

Jones, Ron. "DPMA Model Curriculum to Push Business." Computer World (November 3, 1980), p. 6.

Kam, John B., and Jeffrey D. Ullman. "A Model of Statistical Databases and Their Security." Database Systems, Vol. 2 (March 1977), pp. 1-10.

Kinne, Harold C. "Personal Computers: An Executives Best Friend?" Today's Office (November 1982), p. 68.

Knapp, Thomas J. "Selling Data Security to Upper Management." Data Management (July 1983), pp. 22-25.

Koehn, H. E. "What the Privacy Act Means to Business." Journal of Systems Management, Vol. 26 (June 1975), pp. 12-13.

Linden, T. A. "Operating System Structures to Support Security and Reliable Software." Computing Surveys, Vol. 8 (December 1976), pp. 409-445.

Lobel, J. "Planning a Secure System." Journal of Systems Management (July 1976), pp. 14-19.

Lord, K. W. "Data Center Security: A Case for the Private Eye." Infosystems, Vol. 23 (November 1976), pp. 30-31.

Loston, Adena Williams. "New Curriculum Needed for Prospective Office Managers." Business Education Forum (December 1981), p. 8.

Lowe, T. C. "Computer Security Safeguards or Privacy: The Technical Role in NBS." Bulletin Journal American Society Information Science, Vol. 3, No. 1 (October 1976), pp. 16-18.

Madnick, Stuart E. Report CISR-8, SLOANWP-771-7. Massachusetts: Mass. Institute of Technology, Center for Information Systems Research, March 3, 1975.

Martin, Roy, J. Wayne Spence, and Steve Guynes. "Information Systems Education: An Applied Approach." The Journal of Data Education, Vol. XXI, No. 3 (April 1981), p. 19.

"Maryland Department Loses Computer in Theft." The Chronicle of Higher Education (January 11, 1984), p. 14.

McLean, Gary N. "Curriculum Implications of the Office of the Future . . . or Projected Implications--More (or Less) Accurate." Journal of Business Education (April 1981), p. 268.

Meissner, Paul. "Evaluation of Techniques for Verifying Personal Identity." Proceedings ACM-NBS Fifteenth Annual Technical Symposium, Gaithersburg, MD: June 17, 1976. Washington, DC: Association for Computing Machinery, 1976, pp. 119-127.

Meissner, Paul. "Preventing Unauthorized Use of Systems." Data Processing, Vol. 19 (July/August 1977), pp. 42-43.

Menkus, B. "Protecting Information Assets." Security Management, Vol. 10 (July 1976), pp. 30-32.

Milligan, R. H. "Management Guide to Computer Protection." Journal of Systems Management, Vol. 27 (November 1976), pp. 14-18.

Nunamaker, Jay F., J. Daniel Couger, and Gordon B. Davis, Eds. "Information Systems Curriculum Recommendations for the 80's. Undergraduate and Graduate Programs." Communications of the ACM, Vol. 16, No. 11 (November 1982), p. 781.

Olivas, Louis. "Projections for Our Changing Workplace and Work Force: Implication for Business Educators." Business Education Forum (April 1981), p. 3.

Owens, Bill. "Business Education Implications of Office Automation." The Balance Sheet (September-October 1982), p. 12.

Parker, Donn B. Computer Security Management. Reston, VA: Reston Publishing Co., Inc., 1981.

Parker, Donn B. Crime by Computer. New York: Schribner and Sons, 1976.

Pierson, Joan K. "Business Schools Parallel Model Curriculum in Content." Data Management (February 1984), pp. 42-43.

Pomertanz, F. "Securing the Computer." Data Management, Vol. 12 (June 1974), pp. 18-21.

Potter, George B. Data Processing: An Introduction. Plains, TX: Business Publications, Inc., 1984.

Price, Don. "Update on Business Information Systems Curriculum--DPMA Support Essential to Schools, Industry Acceptance." _Data Management_, Vol. 18, No. 8 (August 1980), pp. 34-35.

Prince, Jeffrey S. "What It Will Take To Manage in the '80's." _Administrative Management_ (February 1980), pp. 34-35.

Ralston, Anthony, and Edwin D. Reilly, Jr. _Encyclopedia of Computer Science and Engineering_. 2nd Ed. New York: Van Nostrum Reinhold Co., 1983.

Ruthberg, Zella G. "Audit and Evaluation of Computer Security." _Proceedings of the NBS Invitational Workshop, Miami Beach, Florida, March 22-24, 1977_. Washington DC: Institute for Computer Sciences and Technology, October 1977.

Schmidt, Patti. "Evaluating Back-up Services." _Data Management_ (July 1983), pp. 30-31.

Schultz, Brad. "ACM Committee Cites Lack of University DP Programs." _Computerworld_ (November 5, 1979), p. 9.

Scoma, L., Jr. "Data Center Security." _Data Management_, Vol. 13 (September 1975), pp. 19-21.

"Security Advice for Execs." _COMP-U-FAX_ (The Corporate Information Resource Newsletter), Vol. 10, No. 5 (November 1983), pp. 1-2.

"Security Software Doubles Your Protection." _Computer Decisions_ (September 1983), p. 46.

Simkin, Mark G. "Is Computer Crime Important." _Journal of Systems Management_, Vol. 33, No. 5 (May 1982), pp. 34-38.

Sippl, Charles J., and Charles P. Sippl. _Computer Dictionary and Handbook_. Indianapolis, IN: Howard W. Sams and Co., Inc., 1972.

Smith, August W. "Data Processing Security: A Common Sense Approach." _Data Management_, Vol. 15 (May 1977), pp. 7-13.

Souder, H. Ray, and David R. Adams. "Survey Reveals Model Curriculum Impact in Academia." _Data Management_ (February 1984), pp. 40-41.

Spence, J. Wayne, Jarrell C. Grout, and John W. Anderson. "What University Business School Graduates Should Know About Computers: A Comparative Study." _Data Management_, Vol. 19, No. 2 (February 1981), pp. 25-29.

SPSS-X User's Guide, A Complete Guide to SPSS-X Language and Operations. New York: McGraw-Hill Book Co., 1983.

Sykes, D. J. "Protecting Data by Encryption." _Datamation_, Vol. 22 (August 1976), p. 81.

Sykes, David. "Enhancing Data Security." Data Comm User (January 1977), pp. 25-28.

Srinivasan, Cadambi A., and Paul E. Dascher. Infosystems, Vol. 28, No. 5, Part 1 (May 1981), pp. 1165-123.

"Teleconferencing--Whose Failure is it, Anyway?" Computer Decisions (October 1983), p. 92.

Thomas, Violet, Dexter R. Schubert, and Jo Ann Lee. Records Management . . . Systems and Administration. New York: John Wiley and Sons, 1983.

University Computer Center User Manual. 2nd Ed. Stillwater, OK: Oklahoma State University, January 1, 1984.

Vanecek, Michael T., and Carl Stephen Guynes. "Business Computer Information Systems DPMA vs ACM: Now What?" Interface: The Computer. Education Quarterly, Vol. , Issue 4 (Winter 1981-82), p. 18.

Ware, Willis H. "Computer Technology: For Better or Worse?" (Paper presented at the National Bureau of Standards Conference on Trends in Applications 1977: Computer Security and Integrity, Washington, DC, May 19, 1977.) Santa Monica, CA: Rand Corporation, July, 1977.

Weber, Austin. "Survey Indicates Data Vulnerability." COMP-U-FAX (The Corporate Information Resource Newsletter), Vol. 10, No. 5 (November 1983), pp. 1-2.

Weik, M. Standard Dictionary of Computers and Information Processing. 2nd Ed. Rochelle Park: Hayden Book Co., 1977.

Woolridge, Susan. Security Standards for Data Processing. New York: Wiley Publishing Co., 1973.

Wroblewski, Michael E. "Contingency Planning for Data Processing." Data Management (May 1982), pp. 24-26.

APPENDICES

APPENDIX A

COMPUTER SECURITY: A MANAGER'S GUIDE

ESTABLISHING A COMPUTER SECURITY PROGRAM

The Need for Computer Security

In the 30 years that electronic computers have been in commercial use, they have completely changed the way most business and government organizations operate. The explosive growth in the use of powerful yet inexpensive microcomputers in recent years promises to make computer-processed information even more central to the functioning of all organizations, not just the largest. Yet as we make the transition to an information-based society, many organizations and managers are simply not aware of the need to protect the information--and the information-processing systems (both hardware and software)--which are their life-blood.

When an organization's computer systems are "down," many of its business activities will cease to function unless adequate provision for alternative processing has been made. If this downtime is extended, the organization's survival may be at stake. Equally important are controls over the information which is processed and stored in computer systems. It is vitally important to prevent unauthorized access to your files and to detect improper use, modification, or destruction of your data. Your information may well be one of your most valuable assets, even more important than your organization's customers, property, or "hard" assets.

Thus you must recognize at the outset that establishing a computer security program will not be easy. There will be resistance from people who don't understand what you are doing, and you will have to educate them to the need for security. And no matter how technically excellent a computer security program you may establish, it will not function with proper effectiveness unless it has the support of both top management and the broad end-user community.

With that in mind, let's turn to a useful though simplified description of the major steps to take in starting a program of computer security in your organization.

STARTING THE PROGRAM

Assign Responsibility

Choose an individual to serve as EDP systems security officer with overall responsibility for EDP security. If your company is small or medium size, you probably will not have someone handle this responsibility on a full-time basis. However, assignment of this role is essential.

Perform a Risk Analysis

Before corrective action can be taken, make a thorough analysis of your risk exposures:

*Identify vulnerabilities and threats. What effect would a disruption of EDP operations have on your company? What would be the effect of loss or destruction of vital records? What about the disclosure of trade secrets or other proprietary data? After all loss potentials are identified, evaluate the threats that could produce those losses . . . fire, power failure, flood, communication and air conditioning malfunctions, unethical employees, unintentional errors by local employees.

*Estimate probabilities of occurrence. What are the chances of these hazards occurring? For some threats, estimating can be relatively easy, e.g., fire, tornado, power outage. Others can be more difficult as in the case of fraud and sabotage.

*Quantify and prioritize loss potential. This final exercise attaches dollar values to the loss potentials previously identified thus making it easier to evaluate, compare, and prioritize.

Conduct a Cost/Benefit Analysis

The risk analysis output ties directly into the evaluation of various risk reducing alternatives. How do you determine whether a proposed security system or procedure is cost-effective? By comparing the cost of the alternative to the potential loss it is expected to reduce or eliminate. Rational decisions can now be made as to the appropriateness of physical access control systems, back-up power, fire protection and other remedial alternatives.

Determine Insurance Requirements

When protection systems and control procedures do not reduce the risk to an acceptable level, the residual risk is transferred to an insurance underwriter. With the results of the risk analysis, you will be in a position to make an intelligent judgement on the amount of insurance required.

Establish a Disaster Recovery Plan

Even after prudent measures have been taken, there exists the possibility of a breach in security. You need a contingency plan to establish a state of preparedness, and a capability to react immediately in a controlled and methodical way. Tasks should be clearly defined, rank-ordered in terms of priority, and they should be well documented and well practiced.

Monitor the Safeguards

Once you have accomplished all of the above tasks, a monitoring mechanism should be instituted. It should verify that control procedures are operable and the various automatic security systems are in working order and capable of performing when called upon.

IN A NUTSHELL

In short, keeping the "big picture" in focus requires a clear understanding of the role data processing plays in supporting day-to-day operations . . . and an understanding that its loss could be catastrophic. Prudent measures must be taken to assure smooth and uninterrupted operation of the EDP function. When you're dealing with hundreds of thousands or millions of dollars worth of assets, the patchwork, piecemeal approach to computer security is not good enough. An effective program does not happen by chance. It requires detailed, time-consuming planning, funding, and a commitment from all levels within the organization. However, if done conscientiously, and with the blessing of top management, it will result in the most efficient use of resources and minimal "surprises."

20 KEY QUESTIONS YOU SHOULD BE ASKING

To get a feel for how well you are now protecting your informational assets, here's a list of useful security questions.

*Is access to your computer room, tape-disc library and forms storage areas denied to personnel other than those who have a business need to enter?

*Does at least one person function as librarian on each shift, and is that person responsible for maintaining up-to-date library records and enforcing data file access controls?

*Is there any centralized control over the selection, acquisition, and use of personal computers and micro software within your organization?

*Are external labels affixed to all tapes and disc packs, and random samples periodically taken to verify that the label properly identifies the contents?

*Are data processing employees prohibited from initiating original accounting transactions, adjustments, corrections?

*Have you identified individual programmers or other technical personnel who are in a position to inflict significant harm to the organization or on whom the organization is excessively dependent?

*Do employees take scheduled vacations to provide an opportunity to expose unauthorized practices?

*Overall, do management policies and practices demonstrate a genuine concern for personnel welfare?

*Do you know who in your organization is using personal computers to access data which is maintained at your central computer facility?

*What protection is afforded organization data which is downloaded from your mainframe to distributed minis and micros? Are local access controls adequate? What about control over reports, floppy disks, etc.?

*Do you use a formal change procedure requiring dual signature authorizations to control systems applications software and modifications?

*Would the organization prosecute employees found guilty of a serious premeditated criminal act against the organization?

*Is an automatic fire extinguishing system installed in the computer room, forms storage room, tape-disc library?

*Is your internal audit function well versed in computer controls and security, and does it work closely with computer security personnel to improve the overall security program?

*For all major financial applications, is there an audit trail diagram and/or description clearly indicating how a transaction may be traced through the system?

*Does internal auditing and/or the security function receive standardized reports of cash and inventory differences, high-dollar transactions, large inventory usages and other unusual, inconsistent or suspicious activity?

*Do customer files contain decoy names and addresses for the purpose of detecting unauthorized use of those files?

*Have you completed a disaster recovery plan . . . has it been given a full-scale test . . . and did it work?

*Does backup planning include the identification of all critical data, programs and documentation that would be necessary to support essential tasks during a disaster recovery period?

*As your computer systems (both hardware and software) change over time, are your security programs and contingency plans revised accordingly?

APPENDIX B

DPMA (DATA PROCESSING MANAGEMENT ASSOCIATION)

MODEL CURRICULUM

APPENDIX B

DPMA (DATA PROCESSING MANAGEMENT ASSOCIATION) MODEL CURRICULUM

Required Courses:

CIS1: Introduction to Computer-Based Systems. A general computer education course for all students at the lower division.

CIS2: Applications Program Development I. Introduction to COBOL at the lower division.

CIS3: Applications Program Development II. Advanced COBOL at the lower division.

CIS4: System Analysis Methods. An introduction to the systems life cycle at the lower division.

CIS5: Structured Systems Analysis and Design. Advanced systems design at the upper division.

CIS6: Database Program Development. Introduction to database management systems at the upper division.

CIS7: Applied Software Development Project. A capstone course with a comprehensive systems development project.

Supporting Courses (all upper division):

CIS8: Software and Hardware Concepts. A survey of the relationships between hardware architecture, systems software, and applications software.

CIS9: Office Automation. Automation and the office environment.

CIS10: Decision Support Systems. A study of decision support systems theory.

CIS11: Advanced Database Concepts. Data modeling, systems development, and data base administration.

CIS12: Distributed Data Processing. Introduction to distributed systems.

CIS13: EDP Audit and Controls. An introduction to controls and EDP auditing.

CIS14: Information Systems Planning. An introduction to the use of information systems in strategic planning.

CIS15: Information Resource Management. A seminar on the management of the information systems resource.

Business Support Courses:

BUS1: Financial Accounting Principals.

BUS2: Managerial Accounting Principals.

BUS3: Quantitative Methods.

BUS4: Principles of Management.

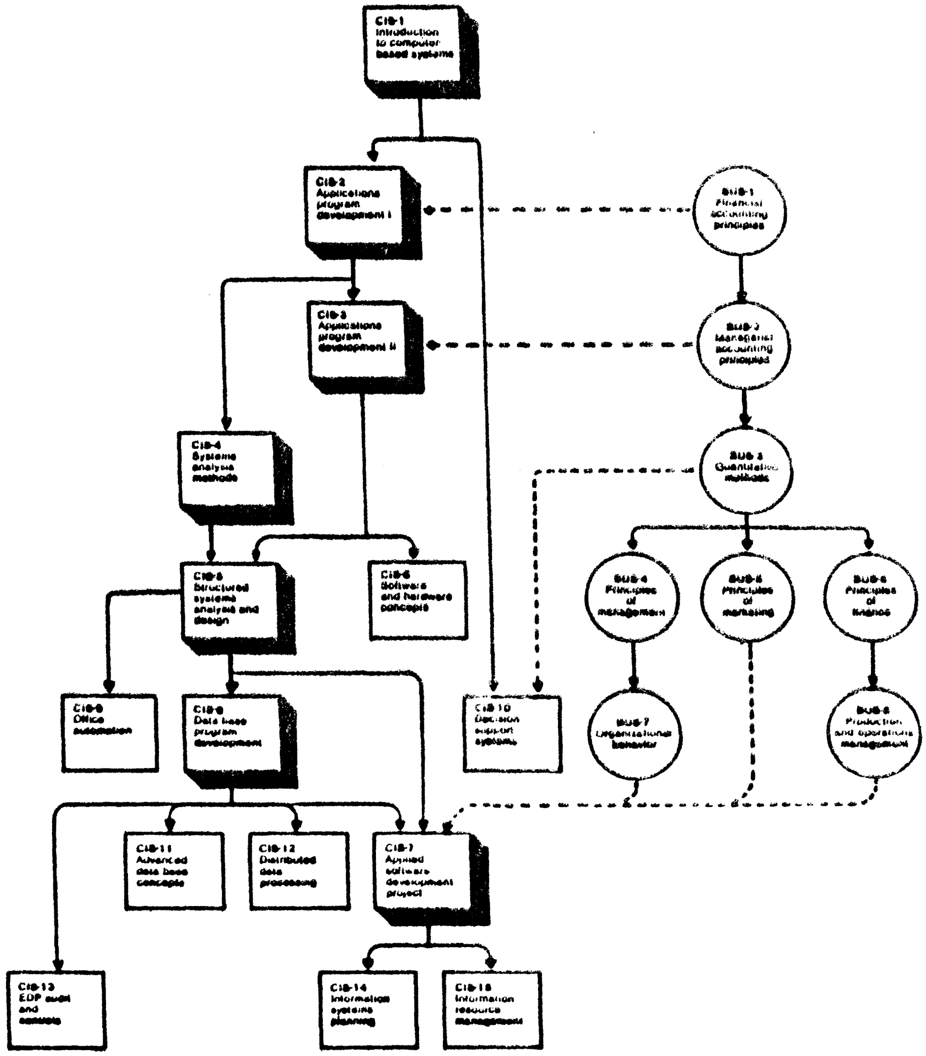
BUS5: Principles of Marketing.

BUS6: Principles of Finance.

BUS7: Organizational Behavior.

BUS8: Production and Operations Management (Vanecek and Guynes, 1981-82).

Structure of DPMA Model Curriculum for Computer Information Systems



Source: Adams and Athey, 1982, p. 15.

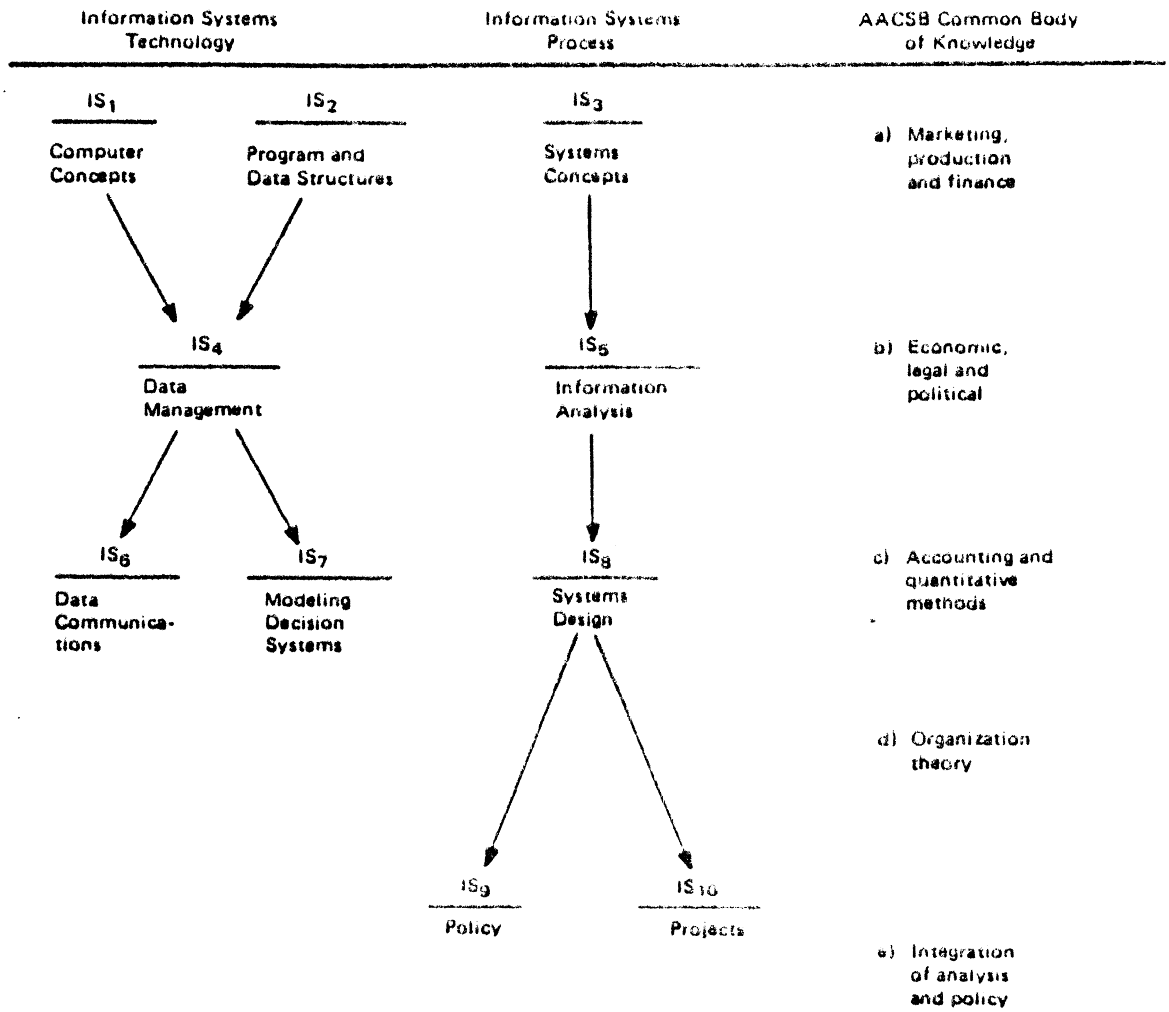
Courses in the DPMA Computer Information Systems Model Curriculum

	CIS core courses	CIS elective courses*	Business support courses**	General Education courses
Freshmen/ Sophomore level	CIS-1, Introduction to computer-based systems CIS-2, Applications program development I CIS-3, Applications program development II CIS-4, Systems analysis methods		BUS-1, Financial accounting principles BUS-2, Managerial accounting principles	Arts Sciences Humanities
Junior/ Senior level	CIS-5, Structured systems analysis and design CIS-6, Data base program development CIS-7, Applied software development project	CIS-8, Software and hardware concepts CIS-9, Office automation CIS-10, Decision support systems CIS-11, Advanced data base concepts CIS-12, Distributed data processing CIS-13, EDP audit and control CIS-14, Information systems planning CIS-15, Information resource management	BUS-3, Quantitative methods BUS-4, Principles of management BUS-5, Principles of marketing BUS-6, Principles of finance BUS-7, Organizational behavior BUS-8, Production and operations management	

*A minimum of three elective courses chosen from this list
**These eight or comparable courses meet minimum requirements

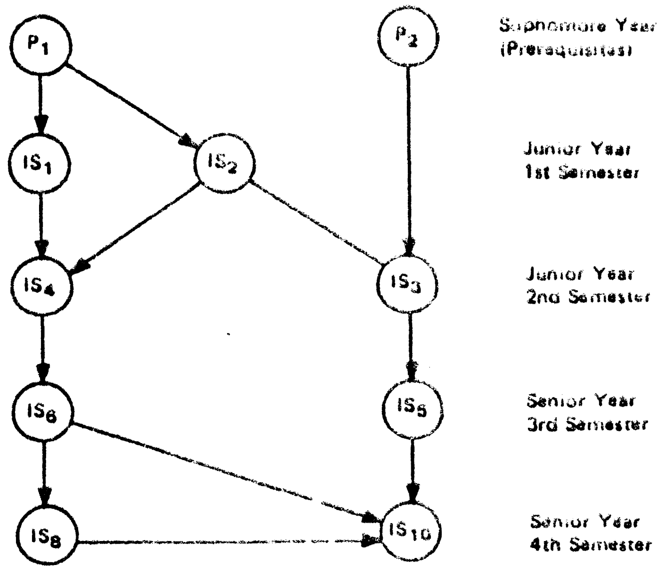
Source: Adams and Athey, 1982, p. 15.

General Structure of Information Systems Curriculum (undergraduate and graduate level)



Source: Nunamaker, Couger, and Davis, November 1982, p. 787.

Undergraduate Level IS Curriculum Structure



Communications
of
the ACM

November 1982
Volume 25
Number 11

Source: Nunamaker, Couger, and Davis, November 1982, p. 787.

APPENDIX C

ACM (ASSOCIATION OF COMPUTER MACHINERY)

MODEL CURRICULUM

APPENDIX C

ACM (ASSOCIATION OF COMPUTER MACHINERY) MODEL CURRICULUM

PREREQUISITES/PREMAJOR/FUNCTIONAL AREA REQUIREMENTS (the AACSB Common Body of Knowledge Courses are at this level):

P1: Computer Programming. Introduce the student to computer programming using a common high-level algorithmic language (implies FORTRAN or PASCAL).

P2: Quantitative Methods. To introduce the concept and use a wide range of analytical models.

Information Systems Technology:

IS1: Computer Systems Concepts. Introduction to hardware and systems software.

IS2: Program, Data, and File Structures. A combination of data structures, file handling, and COBOL (or PL/1) programming.

IS4: Data Management. Introduction to database management systems.

IS6: Data Communications, Networks, and Distributed Processing. Introduces the student to distributed systems and teleprocessing.

IS7: Modeling and Decision Systems. An introduction to modeling and decision support systems.

Information Systems Concept in Organization:

IS3: Systems and Information Concepts in Organizations. Introduction to systems theory, information flow, and the nature of information systems.

IS5: Information Analysis. Introduction to the systems life cycle and systems analysis.

IS8: Systems Design. A rigorous approach to systems design and specification is covered.

IS9: Information System Policy and Administration. Evaluation of administrative and management issues in the information systems function.

IS10: Systems Development Project. Capstone course consisting of a systems development project.

APPENDIX D

PILOT STUDY

Oklahoma State University

COLLEGE OF BUSINESS ADMINISTRATION

STILLWATER, OKLAHOMA 74078
(405) 624-5064

February 13, 1984

Dear:

This is to request your assistance in completing a pilot study of the attached questionnaire concerning data security curriculum considerations.

The target group for this study will be 600 members of the Data Processing Management Association throughout the United States. These members will be randomly selected from approximately 16,000 members in the Data Processing Management or Operations Management category.

Would you please assist us in our attempt to make certain that the cover letter and questionnaire are clear as to purpose and desired response. Your suggestions will be seriously considered before mailing out the questionnaire to the targeted group. Please mark your suggestions or changes directly on the cover letter and questionnaire or attach a separate sheet.

Thank you very much for taking time from your busy schedule to assist us in our research efforts. Your participation is greatly appreciated. A stamped, self-addressed envelope is enclosed for returning your completed response on or before February 27, 1984. If you have any questions, please call me at 405-624-7559.

Cordially,

Karen A. Forcht

Karen A. Forcht

KAF/vet

Enclosure

OKLAHOMA STATE UNIVERSITY

M E M O R A N D U M

DATE February 13, 1984

TO

FROM Karen A. Forcht

SUBJECT Pilot Study Questionnaire

This is to request your assistance in completing a pilot study of the attached questionnaire concerning data security curriculum considerations.

The target group for this study will be 600 members of the Data Processing Management Association throughout the United States. These members will be randomly selected from approximately 16,000 members in the Data Processing Management or Operations Management category.

Would you please assist us in our attempt to make certain that the cover letter and questionnaire are clear as to purpose and desired response. Your suggestions will be seriously considered before mailing out the questionnaire to the targeted group. Please mark your suggestions or changes directly on the cover letter and questionnaire or attach a separate sheet.

Thank you very much for taking time from your busy schedule to assist us in our research efforts. Your participation is greatly appreciated. A stamped, self-addressed envelope is enclosed for returning your completed response on or before February 27, 1984. If you have any questions, please call me at 405-624-7559.

KAF/vet

Enclosure

____
Identification Number

QUESTIONNAIRE ON DATA SECURITY CURRICULA

This questionnaire is a survey of DPMA members to determine opinions concerning inclusion of data security topics into the Computer Information Systems Programs in collegiate schools of business. For the purpose of clarification, computer security may be defined as any activity that involves the functions of avoidance, deterrance, prevention, detection, recovery, and correction of data so that privacy and security of the data and equipment are not violated.

Please complete the questionnaire by checking the appropriate response. Your participation in this survey is greatly appreciated.

I. BUSINESS INFORMATION

This portion of the questionnaire pertains to the use of electronic data processing by your firm.

1. What make and Model of computer do you presently utilize for your operation? (Please list all models used if your organization utilizes more than one).

2. How many people are presently employed in your computer center? (Please check one).

   a. _____1-10 d _____31-40
   b. _____11-20 e. _____41-50
   c. _____21-30 f. _____Over 50

3. Does your computer center have a designated person(s) directly responsible for data security? (Please check one)

   a. _____Yes (If yes, please complete number 4 and 5 below)
   b. _____No (If no, please skip 4 and 5 and complete number 6 below)

4. How many people in your organization are directly responsible for computer security?

   ____

5. Title of person(s) directly responsible for data security. (Please check all that apply).

   a. _____Security Analyst
   b. _____Operations Analyst
   c. _____Director of Data Security
   d. Other (Please specify title)
   ____
   ____

6. Answer this question ONLY if you selected NO in number 3 above. (Please check all that apply).

   a. _____Data Security function is performed as part of other responsibilities and NOT listed as a separate job function.

   b. _____We have no formal program in data security.

   c. _____Consultants are utilized for data security analysis purposes.

   d. _____Other methods of data security analysis are utilized. Please specify below.

II. PERSONAL INFORMATION

This portion of the questionnaire pertains to your personal and educational background.

1. Please indicate your present position:

   a. _____Data Processing Management
   b. _____Operational Management
   c. _____Security Analyst
   d. _____Other (Please specify below)

   ____

2. How long have you been in the position identified in item 1 above?

   a. _____less than 1 year
   b. _____1-2 years
   c. _____3-4 years
   d. _____5-6 years
   e. _____more than 6 years

3. How long have you been employed in a computer-related position (Please include the time in your present position in this total).

   a. _____less than 1 year
   b. _____1-2 years
   c. _____3-4 years
   d. _____5-6 years
   e. _____7-10 years
   f. _____more than 10 years

4. Please indicate your highest educational level.

   a. _____High School Graduate
   b. _____Some college work
   c. _____Associate Degree
   d. _____Vocational/Trade School Certificate
   e. _____Bachelor's Degree
   f. _____Master's Degree
   g. _____Doctoral Degree
   h. _____Other (Please specify in the following space)______________

5. Please indicate if you have utilized any of the following educational or training areas in computer security. (Please check all that apply).

   a. _____Regular college courses or college extension courses
   b. _____In-house training programs presented by a member of your organization
   c. _____Vendor-sponsored seminars
   d. _____Seminars offered by other private companies and presented by a member of their staff
   e. _____Self-education (i.e. independent reading and study)
   f. _____No training/education in data security

6. How many employees do you directly supervise at the present time?

   a. _____none
   b. _____1-5
   c. _____6-10
   d. _____11-15
   e. _____16-20
   f. _____21-25
   g. _____more than 25

7. Please check the data processing professional organization in which you currently hold memberships.

   a. _____DPMA
   b. _____ACM
   c. _____Data Security Institute
   d. _____Other (Please specify)

   ____
   ____
   ____

8. Are you familiar with any of the following Computer Information Systems Model Curriculums?

a. DPMA ______yes ______no
b. ACM ______yes ______no
c. Other ______yes ______no

Please specify other____

III. NEED FOR DATA SECURITY KNOWLEDGE

This portion of the questionnaire requests your opinions concerning the need for data security knowledge by persons employed in computer centers.

1. Do you feel computer center employees should possess some knowledge about computer security?

a. ______yes (if yes, please go to Section IV below)
b. ______no (if no, please answer the following question and then go to Section V on page 6).

2. If your response to number 1 above was no, please answer the following questions. (Please check all that apply).

a. ______It is not necessary for most employees to possess security information in order to efficiently perform their jobs efficiently.
b. ______Data security should be handled only by those who are directly involved in administering security programs.
c. ______Other (Please specify)
____
____
____
____

PLEASE GO TO SECTION V ON PAGE 6.

IV. ANALYSIS OF DATA SECURITY TOPICS
(To be completed ONLY by those respondents who checked yes in number 1 above).

Since you have indicated a "yes" response in Section III, item 1 above, please answer the following questions concerning data security knowledge needed by graduates of Computer Information Systems programs in the collegiate schools of business so that skills and knowledge needed for computer center employees can be determined.

1. Please indicate the importance of the following topic areas that might be considered for inclusion in the Computer Information Systems Curriculum relating to the topic of computer security.

4

Please us the following rating scale:

1 - Very Important
2 - Important
3 - Average Importance
4 - Unimportant
5 - Very unimportant

a. _____Overview of computer security
b. _____Company data security programs
c. _____Embezzlement: Detection and Control
d. _____EDP Controls
e. _____Auditing
f. _____Program Error
g. _____Operator Error
h. _____Programmer Fraud
i. _____Operator Fraud
j. _____Software Protection
k. _____Hardware Protection
l. _____Fire Protection
m. _____Disaster Protection
n. _____Insurance against loss
o. _____Cryptographic Techniques
p. _____Protections when using service bureaus
q. _____Time-sharing protections
r. _____Protection and privacy considerations
s. _____Others (Please list)

____
____
____
____
____
____

2. Which of the following methods do you feel would <u>best</u> develop computer security knowledge?

   a. _____Complete course in data security in addition to incorporation of data security topics in the Computer Information Systems Curriculum.
   b. _____Complete course in data security ONLY.
   c. _____Incorporation of data security topics into the current courses in the Information Processing Curriculum ONLY.
   d. _____Other method (Please specify).

   ____

3. Please indicate your opinion regarding the importance of including elements of Computer Security into the following courses within the CIS Curriculum:

   Course titles and descriptions are taken from <u>DPMA Model Curriculum for Undergraduate Computer Information Systems Education</u>, 1981, pages 11-13.

   Please use the following rating scale:

   1 - Very Important
   2 - Important
   3 - Average Importance
   4 - Unimportant
   5 - Very unimportant

   <u>Core Courses</u>

   a. _____CIS-1 INTRODUCTION TO COMPUTER-BASED SYSTEMS
   ....An introduction to computers and data processing taught as a general education course for all students (lower division).

   b. _____CIS-2 APPLICATIONS PROGRAM DEVELOPMENT I
   ....A beginning computer problem solving and programming course using COBOL as the vehicle language (lower division).

   c. _____CIS-3 APPLICATIONS PROGRAM DEVELOPMENT II
   ....An advanced computer problem solving and programming course using COBOL (lower division).

d. _____CIS-4 SYSTEMS ANALYSIS METHODS
....An overview of the systems development life cycle with emphasis on techniques and tools of system documentation and logical system specifications (lower division).

e. _____CIS-5 STRUCTURED SYSTEMS ANALYSIS AND DESIGN
....Advanced coverage of the strategies and techniques of structured systems development (upper division).

f. _____CIS-6 DATABASE PROGRAM DEVELOPMENT
....A course emphasizing software design and programming in a data-base environment (upper division).

g. _____CIS-7 APPLIED SOFTWARE DEVELOPMENT PROJECT
....A capstone systems course integrating the knowledge and abilities gained through the other computer-related courses in the curriculum within a comprehensive system development project (upper division).

<u>Elective Courses</u>

a. _____CIS-8 SOFTWARE AND HARDWARE CONCEPTS
....A survey of technical topics related to computer systems with emphasis on the relationships between hardware architecture, systems software, and applications software.

b. _____CIS-9 OFFICE AUTOMATION
....An examination of the office as a center of business activity, operational logistics, and decision support, and the impact of automation on the office environment.

c. _____CIS-10 DECISION SUPPORT SYSTEMS
....An analysis of the highest level of information support systems which aid the manager in the decision-making process.

d. _____CIS-11 ADVANCED DATABASE CONCEPTS
....An in-depth investigation of data modeling, system development, and data administration in a database environment.

e. _____CIS-12 DISTRIBUTED DATA PROCESSING
....An examination of the features and impact of distributed systems in the business enterprise.

f. _____CIS-13 EDP AUDIT AND CONTROLS
....An introduction to EDP auditing with emphasis on EDP controls, audit types, and audit techniques and their effects on system development.

g. _____CIS-14 INFORMATION SYSTEMS PLANNING
....An introduction to the financial, technical, and strategic information systems planning process.

h. _____CIS-15 INFORMATION RESOURCE MANAGEMENT
....A seminar in information systems management with emphasis on planning, organizing, and controlling user services and managing the systems development process.

V. OPTIONAL

Name ______________________________

Organization ______________________________

Address ______________________________

____

____

Position ______________________________

* *

Thank you for your participation in this survey. Your input will aid greatly in the analysis of curriculum considerations concerning data security. We appreciate your taking the time to fill out this questionnaire.

Please return the completed questionnaire in the <u>enclosed</u>, <u>stamped</u> envelope to:

Karen A. Forcht, 207 College of Business, Oklahoma State University, Stillwater, Oklahoma 74078 on or before______________________.

* *

VI. ADDITIONAL COMMENTS

Please use the space provided below to add any additional comments and suggestions relating to the questionnaire, the study being conducted, or the the subject of data security. Your comments will be taken into consideration and utilized in our report. When commenting, please refer to the appropriate section number of this questionnaire. Thank you.

OKLAHOMA STATE UNIVERSITY

M E M O R A N D U M

DATE March 15, 1984

TO Questionnaire Respondents

FROM Karen Forcht, Graduate Teaching Associate
Administrative Services and Business Education Department

SUBJECT Questionnaire on Computer Security Curricula

Thank you very much for taking the time to fill out (and in several cases, to discuss) my pilot questionnaire on the topic of Computer Security Curricula. Your input was invaluable in refining the questionnaire and aided me greatly in getting all the "bugs out". The completed questionnaire is ready to mail, and I feel very confident that the study is going to yield some very positive results--thanks to your help.

If you would like an abstract of the results, please note on the bottom of this memo and return to me in the envelope provided.

Oklahoma State University

STILLWATER, OKLAHOMA 74078
(405) 624-5064

COLLEGE OF BUSINESS ADMINISTRATION

March 15, 1984

Recently you returned the pilot questionnaire for our research topic dealing with Computer Security Curricula. Thank you very much for taking time from your busy schedule to add your valuable comments to the questionnaire. It was obvious that many of you were very interested in the topic and your additional comments and suggestions were taken into consideration.

The completed questionnaire is ready to be mailed, and we feel very confident that the questionnaire is going to yield some positive results--thanks to your help.

If you would like an abstract of the results, please note on the bottom of this page and return to us in the envelope provided.

Thank you so much for your assistance in this research project.

Sincerely,

Karen A. Forcht

Karen A. Forcht, Research Associate

Herbert M. Jelley

Herbert M. Jelley, Professor

APPENDIX E

COVER LETTERS AND STUDY INSTRUMENT

Oklahoma State University

COLLEGE OF BUSINESS ADMINISTRATION

STILLWATER, OKLAHOMA 74078
(405) 624-5064

April 6, 1984

Dear DPMA Member:

SUBJECT: COMPUTER SECURITY CURRICULUM SURVEY

During the past decade, as you know, the development and proliferation of computers in organizations of all sizes and functions have increased rapidly. Along with this phenomenal growth, data security violations, both accidental and intentional, have become more prominent. The issue of computer security seems to become even more paramount and complex as our present office environment becomes increasingly more automated. We are currently conducting a survey to determine whether computer center personnel feel college students in Computer Information Systems programs should become more aware of the concerns of computer security.

As a person at the operational or data processing management level, you have been selected from DPMA's mailing list to participate in this study. Would you please take approximately 15 minutes of your time to complete the enclosed questionnaire and return it in the stamped envelope provided. Your input will aid greatly in the assessment of our current college curriculum in the Computer Information Systems area. We would like to keep pace with industry's employment requirements, and this study will assist us in updating our programs.

Thank you very much for your participation in this study. Please indicate if you wish to have an abstract of the completed research.

Cordially,

Karen A. Forcht

Karen A. Forcht, Research Associate

Herbert M. Jelley

Herbert M. Jelley, Professor

Enclosure

P.S. The Identification Number on the questionnaire will be used for follow-up purposes only. You may be assured that the results of questionnaire will be completely confidential.

Oklahoma State University

COLLEGE OF BUSINESS ADMINISTRATION

STILLWATER, OKLAHOMA 74078
(405) 624-5064

May 7, 1984

Dear DPMA Member:

SUBJECT: FOLLOW-UP ON COMPUTER SECURITY CURRICULUM SURVEY

Recently you received a questionnaire requesting your opinions concerning computer security topics. We are interested in learning whether computer center personnel feel college students in Computer Information Systems programs should become more aware of the concerns of computer security.

At the time this letter was mailed, a response had not been received from you. We would greatly appreciate your taking a few minutes to complete the enclosed questionnaire and return it to us by June 1, 1984 in the envelope provided. If the equestionnaire has since been completed and returned, we sincerely thank you for your participation.

Your participation will add greatly to the results of this vital study. We sincerely appreciate your efforts. Please indicate if you wish to have an abstract of the completed research.

Cordially,

Karen A. Forcht

Karen A. Forcht, Research Associate

Herbert M. Jelley

Herbert M. Jelley, Professor

Enclosure

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY MAIL

FIRST CLASS PERMIT NO. 366 STILLWATER, OK

POSTAGE WILL BE PAID BY ADDRESSEE

CENTRAL MAILING SERVICES
STILLWATER, OKLAHOMA 74078

Karen A. Forcht
1-1-33050-6010

Karen A. Forcht

Oklahoma State University

COLLEGE OF BUSINESS ADMINISTRATION
STILLWATER, OKLAHOMA 74078

1-1-33050-6010, 2302

IDENTIFICATION NUMBER

QUESTIONNAIRE ON DATA SECURITY CURRICULA

This questionnaire is a survey of selected DPMA members to determine opinions concerning inclusion of computer security topics into the Computer Information Systems (CIS) Programs in collegiate schools of business. For the purpose of clarification, computer security may be defined as any activity that involves the functions of avoidance, deterrance, prevention, detection, recovery, and correction of data so that privacy and security of the data and equipment are not violated.

Please complete the questionnaire by checking the appropriate response. Your participation in this survey is greatly appreciated.

I. BUSINESS INFORMATION

This portion of the questionnaire pertains to the use of electronic data processing by your firm.

1. What make and model of computer do you presently utilize for your operation? (Please list all models used if your organization utilizes more than one).

IBM ______	NCR ______	Others ______
Burroughs ______	Apple ______	______
Hewlett Packard ______	Radio Shack ______	______

2. How many people are presently employed in your computer center? (Please check one).

a. ______1-20	c. ______41-60	e. ______81-100
b. ______21-40	d. ______61-80	f. ______Over 100
		Please specify number ______

3. Does your computer center have a designated person(s) directly responsible for computer security? (Please check one)

   a. ______Yes (If yes, please complete number 4 and 5 below)
   b. ______No (If no, please skip 4 and 5 and complete number 6 below)

4. How many people in your organization are DIRECTLY responsible for computer security as stated in their job description? ______

5. Title of person(s) directly responsible for computer security. (Please check all that apply).

   a. ______Security Analyst
   b. ______Operations Analyst
   c. ______Director of Computer Security
   d. Other (Please specify title) ______

6. Answer this question ONLY if you selected NO in number 3 above. (Please check all that apply).

   a. ______Computer Security function is performed as part of other responsibilities and NOT listed as a separate job function.
   b. ______We have no formal program in computer security.
   c. ______Consultants are utilized for computer security analysis purposes.
   d. ______Other methods of computer security analysis are utilized. Please specify below.

   ______

II. PERSONAL INFORMATION

This portion of the questionnaire pertains to your personal and educational background.

1. Please indicate your present position:

   a. _____Data Processing Management
   b. _____Operational Management
   c. _____Security Analyst
   d. _____Other (Please specify below)

   ____

2. How long have you been in your present position?

   a. _____less than 1 year
   b. _____1-2 years
   c. _____3-4 years
   d. _____5-6 years
   e. _____more than 6 years

3. How long have you been employed in a computer-related position (Please include the time in your present position in this total).

   a. _____less than 1 year
   b. _____1-2 years
   c. _____3-4 years
   d. _____5-6 years
   e. _____7-10 years
   f. _____more than 10 years

4. Please indicate your highest educational level.

   a. _____High School Graduate
   b. _____Some college work. Specify major ______________
   c. _____Associate Degree. Specify major ______________
   d. _____Vocational/Trade School Certificate. Specify major ______________
   e. _____Bachelor's Degree. Specify major ______________
   f. _____Master's Degree. Specify major ______________
   g. _____Doctoral Degree. Specify major ______________
   h. _____Other (Please specify in the following space)______________

5. Please indicate if you have utilized any of the following educational or training areas in COMPUTER SECURITY. (Please check all that apply).

   a. _____Regular college courses or college extension courses
   b. _____In-house training programs presented by a member of your organization
   c. _____Seminars offered by other private companies and presented by a member of their staff, including vendor-sponsored seminars
   d. _____Self-education (i.e. independent reading and study)
   e. _____No training/education in data security

6. How many employees do you directly supervise at the present time?

   a. _____none
   b. _____1-5
   c. _____6-10
   d. _____11-15
   e. _____16-20
   f. _____21-25
   g. _____more than 25

7. Please check the data processing professional organization(s) in which you currently hold memberships. (Please check all that apply).

   a. _____DPMA
   b. _____ACM
   c. _____Data Security Institute
   d. _____Other (Please specify)

   ____
   ____
   ____

8. Are you familiar with any of the following Computer Information Systems Model Curriculums?

   a. DPMA ______yes ______no
   b. ACM ______yes ______no
   c. Other ______yes ______no

   Please specify other____

III. NEED FOR COMPUTER SECURITY KNOWLEDGE

This portion of the questionnaire requests your opinions concerning the need for computer security knowledge by persons employed in computer centers.

1. Do you feel computer center employees should possess some knowledge about computer security?

   a. ______yes (If yes, please go to Section IV below)
   b. ______no (If no, please answer the following question and then go to Section V on page 6).

2. If your response to number 1 above was no, please answer the following statements. (Please check all that apply).

   a. ______It is not necessary for most employees to possess security information in order to efficiently perform their jobs.
   b. ______Computer security should be handled only by those who are directly involved in administering security programs.
   c. ______Other (Please specify)
      ____
      ____
      ____
      ____

PLEASE GO TO SECTION V ON PAGE 6.

IV. ANALYSIS OF COMPUTER SECURITY TOPICS

(To be completed ONLY by those respondents who checked yes in number 1 above).

Since you have indicated a "yes" response in Section III, item 1 above, please answer the following questions concerning computer security knowledge needed by graduates of Computer Information Systems programs in the collegiate schools of business so that skills and knowledge needed for computer center employees can be determined.

1. Please indicate the importance of the following topic areas that might be considered for inclusion in the Computer Information Systems Curriculum relating to the topic of computer security.

Please use the following rating scale:

1 - Very Important
2 - Important
3 - Average Importance
4 - Unimportant
5 - Very unimportant

a. _____Overview of computer security
b. _____Company computer security programs
c. _____Embezzlement: Detection and control
d. _____EDP controls and Auditing
e. _____Program error
f. _____Operator error
g. _____Programmer fraud
h. _____Operator fraud
i. _____Software protection
j. _____Hardware protection
k. _____Fire protection
l. _____Disaster protection
m. _____Insurance against loss
n. _____Cryptographic techniques
o. _____Protections when using service bureaus
p. _____Time-sharing protections
q. _____Protection and privacy considerations
r. _____Security Software Packages (i.e. RACF)
s. _____Others (Please List)

2. Which of the following methods do you feel would best develop computer security knowledge?

a. _____Complete course in computer security in addition to incorporation of computer security topics in the Computer Information Systems Curriculum.
b. _____Complete course in computer security ONLY.
c. _____Incorporation of computer security topics into the current courses in the Computer Information Systems (CIS) Curriculum ONLY.
d. _____Other method (Please specify).

3. Please indicate YOUR OPINION regarding the importance of including elements of Computer Security into the following courses within the CIS Curriculum:

Course titles and descriptions are taken from DPMA Model Curriculum for Undergraduate Computer Information Systems Education, 1981, pages 11-13.

Please use the following rating scale:

1 - Very Important
2 - Important
3 - Average Importance
4 - Unimportant
5 - Very unimportant

Core Courses

a. _____CIS-1 INTRODUCTION TO COMPUTER-BASED SYSTEMS
....An introduction to computers and data processing taught as a general education course for all students (lower division).

b. _____CIS-2 APPLICATIONS PROGRAM DEVELOPMENT I
....A beginning computer problem solving and programming course using COBOL as the vehicle language (lower division).

c. _____CIS-3 APPLICATIONS PROGRAM DEVELOPMENT II
....An advanced computer problem solving and programming course using COBOL (lower division).

5

d. ______CIS-4 SYSTEMS ANALYSIS METHODS
....An overview of the systems development life cycle with emphasis on techniques and tools of system documentation and logical system specifications (lower division).

e. ______CIS-5 STRUCTURED SYSTEMS ANALYSIS AND DESIGN
....Advanced coverage of the strategies and techniques of structured systems development (upper division).

f. ______CIS-6 DATABASE PROGRAM DEVELOPMENT
....A course emphasizing software design and programming in a data-base environment (upper division).

g. ______CIS-7 APPLIED SOFTWARE DEVELOPMENT PROJECT
....A capstone systems course integrating the knowledge and abilities gained through the other computer-related courses in the curriculum within a comprehensive system development project (upper division).

Elective Courses

a. ______CIS-8 SOFTWARE AND HARDWARE CONCEPTS
....A survey of technical topics related to computer systems with emphasis on the relationships between hardware architecture, systems software, and applications software.

b. ______CIS-9 OFFICE AUTOMATION
....An examination of the office as a center of business activity, operational logistics, and decision support, and the impact of automation on the office environment.

c. ______CIS-10 DECISION SUPPORT SYSTEMS
....An analysis of the highest level of information support systems which aid the manager in the decision-making process.

d. ______CIS-11 ADVANCED DATABASE CONCEPTS
....An in-depth investigation of data modeling, system development, and data administration in a database environment.

e. ______CIS-12 DISTRIBUTED DATA PROCESSING
....An examination of the features and impact of distributed systems in the business enterprise.

f. ______CIS-13 EDP AUDIT AND CONTROLS
....An introduction to EDP auditing with emphasis on EDP controls, audit types, and audit techniques and their effects on system development.

g. ______CIS-14 INFORMATION SYSTEMS PLANNING
....An introduction to the financial, technical, and strategic information systems planning process.

h. ______CIS-15 INFORMATION RESOURCE MANAGEMENT
....A seminar in information systems management with emphasis on planning, organizing, and controlling user services and managing the systems development process.

V. OPTIONAL

Name ______________________________

Organization ______________________________

Address ______________________________

____

____

Position ______________________________

* *

Thank you for your participation in this survey. Your input will aid greatly in the analysis of curriculum considerations concerning computer security. We appreciate your taking the time to fill out this questionnaire.

Please return the completed questionnaire in the enclosed, stamped envelope to:

Karen A. Forcht, 207 College of Business, Oklahoma State University, Stillwater, Oklahoma 74078 on or before May 1, 1984.

* *

VI. ADDITIONAL COMMENTS

Please use the space provided below for any additional comments and suggestions relating to the questionnaire, the study being conducted, or the the subject of computer security. Your comments will be taken into consideration and utilized in our report. When commenting, please refer to the appropriate section number of this questionnaire. Thank you.

APPENDIX F

DATA PROCESSING MANAGEMENT ASSOCIATION

MAILING LIST

Oklahoma State University

COLLEGE OF BUSINESS ADMINISTRATION

STILLWATER, OKLAHOMA 74078
(405) 624-5064

January 20, 1984

Ms. Delores Thell
Data Processing Management Association
505 Busse Highway
Park Ridge, Illinois 60068-3191

Dear Ms. Thell:

Thank you for your assistance recently during our telephone conversation concerning a possible mailing list for my doctoral dissertation. As per our conversation, I would like to request the following mailing list of DPMA members to be used for my doctoral dissertation questionnaire mailing:

1. Two (2) sets of pressure sensitive labels

   --700 names on list
   --One listing will be for the original mailing and one for the follow-up mailing. Both sets should contain the same listing of names.
   --U. S. Members only
   --The listing should be randomly drawn from the total populace of this grouping.

2. Please extract listing from:

   --Job Function category B ONLY (Data Processing and Operational Management)
   --No code is needed on the label so please omit.

I have enclosed a personal check in the amount of $100.00, which is the price you quoted for the above mailing list. If additional monies are required, please let me know.

Please call me at 405--624-0842 (H) or 405--624-7559 (O) if you have any questions concerning the above.

Please send the labels to my office address at:

Room 207, College of Business Administration, Oklahoma State University, Stillwater, OK 74075

I have enclosed a copy of my approved dissertation proposal for your information. Please refer to page 20 concerning how the mailing list will be used. Thank you for your assistance. I will send the questionnaire as soon as it is approved.

Cordially,

Karen A. Forcht

Karen A. Forcht, Graduate Teaching Associate

enc.

MEMO

Data Processing
Management
Association

505 Busse Hwy.
Park Ridge, Ill.
60068
(312)825-8124

Dear Ms. Forcht:

Your order was for 700 labels each. Because we "salt" our list, you will find that actually you have 952 labels each. The additional names, I'm sure, are mostly data processing and operational managers. However, if you would like to omit the "salted list", just omit any names that begin with D M. Since you are sending out a survey, you may not want to use these additional names.

5 Busse Highway, Park Ridge, Illinois 60068
(312)825-8124

DP& Op Prgs. 2 sets labels 700 each
to Karen A. Forcht

Data Processing Management Association

IMPORTANT NOTICE

DPMA has agreed to furnish you with these labels on a rental basis only. The fee you have paid is for a ~~one~~ two time usage only for the specific mailing item(s) of which you submitted a sample to us for our approval. These labels are entered randomly in our list to review the actual mailings sent out. Any violation of this rental agreement will be followed up immediately by our legal counsel.

To insure the fact that you understand the given conditions would you please sign and return this notice.

- -

3-16-84

Company Name Okla. State Univ.

Name Karen A. Forcht Title Grad Res Associate

Order Number Unknown

Karen A. Forcht
2622 N. Park Drive
Stillwater, OK 74075

Karen A. Forcht

The Association Of Information Processing And Computer Management

APPENDIX G

MEANS OF ADDITIONAL COMPUTER SECURITY TOPICS

APPENDIX G

MEANS OF ADDITIONAL COMPUTER SECURITY TOPICS

The top five topics were chosen from the listing of 19 topics. Analysis of these top five topics is given in Section IV. These remaining topics are listed in the same order that was used in Section IV to facilitate ease of interpretation.

TABLE LXIV

SIZE OF COMPUTER CENTER COMPARED TO SELECTED TOPICS

	Mean	Std Dev	Cases
	Topic B - Company Computer Security Programs		
	3.9032	.9685	248
1-20	3.7643	1.0080	140
21-40	3.8649	.9178	37
41-60	4.1000	.8522	20
61-80	4.0000	.6325	6
81-100	4.1538	.8987	13
over 100	4.3125	.8958	32
	Topic C - Embezzlement: Detection and Control		
	3.4960	1.0377	248
1-20	3.5000	1.0628	140
21-40	3.5946	1.0127	37
41-60	3.3500	1.0894	20
61-80	3.8333	.7528	6
81-100	3.3846	.7679	13
over 100	3.4375	1.1053	32
	Topic E - Program Error		
	3.5927	.9936	248
1-20	3.6643	1.0221	140
21-40	3.7838	.8211	37
41-60	3.5500	1.1910	20
61-80	2.8333	.7528	6
81-100	3.3846	.9608	13
over 100	3,3125	.8958	32
	Topic F - Operator Error		
	3.5927	.9689	248
1-20	3.6214	1.0069	140
21-40	3.8108	.8110	37
41-60	3.5000	1.1002	20
61-80	3.0000	.6325	6
81-100	3.4615	.8771	13
over 100	3.4375	.9483	32

TABLE LXIV (Continued)

	Mean	Std Dev	Cases
	Topic G - Programmer Fraud		
	3.7137	1.0234	248
1-20	3.6786	1.1011	140
21-40	3.8378	1.0412	37
41-60	3.7000	.8645	20
61-80	3.5000	.5477	6
81-100	3.8462	.8006	13
over 100	3.7188	.9240	32
	Topic H - Operator Fraud		
	3.6694	1.0395	248
1-20	3.6571	1.0847	140
21-40	3.7838	1.0037	37
41-60	3.6000	.9947	20
61-80	3.5000	.5477	6
81-100	3.9231	.8623	13
over 100	3.5625	1.0758	32
	Topic J - Hardware Protection		
	3.9718	.9325	248
1-20	4.0000	.9291	140
21-40	4.1892	.8768	37
41-60	3.8500	.9333	20
61-80	3.5000	.5477	6
81-100	3.7692	.8321	13
over 100	3.8438	1.0809	32
	Topic M - Insurance Against Loss		
	3.4073	1.1201	248
1-20	3.3857	1.1727	140
21-40	3.3784	1.0097	37
41-60	3.7000	.6569	20
61-80	3.5000	.8367	6
81-100	3.5385	1.5064	13
over 100	3.2813	1.1426	32

TABLE LXIV (Continued)

	Mean	Std Dev	Cases
	Topic N - Cryptographic Techniques		
	2.7339	1.0347	248
1-20	2.6571	1.0578	140
21-40	2.6216	1.0633	37
41-60	3.0500	.9445	20
61-80	3.0000	1.0954	6
81-100	2.7692	.7250	13
over 100	2.9375	1.0453	32
	Topic O - Protections When Using Service Bureaus		
	3.4534	1.0461	247
1-20	3.5143	1.0761	140
21-40	3.3784	1.0633	37
41-60	3.3500	1.0400	20
61-80	3.3333	.8165	6
81-100	3.5385	1.0500	13
over 100	3.3226	.9794	31
	Topic P - Time-Sharing Protections		
	3.7166	1.0518	247
1-20	3.6835	1.0970	139
21-40	3.8649	1.0045	37
41-60	3.7000	.9234	20
61-80	4.0000	1.0954	6
81-100	4.0005	.9129	13
over 100	3.5313	1.0468	32
	Topic Q - Protection and Privacy Considerations		
	3.7742	.9768	248
1-20	3.7000	1.0086	140
21-40	3.8919	.9656	37
41-60	3.5500	.8256	20
61-80	4.1667	.9832	6
81-100	4.5385	.6602	13
over 100	3.7188	.8514	32

TABLE LXIV (Continued)

	Mean	Std Dev	Cases
	Topic R - Security Software Packages		
	3.2163	.9783	245
1-20	3.0217	.9776	138
21-40	3.5278	.8779	36
41-60	3.4500	.8870	20
61-80	3.8333	.7528	6
81-100	3.2308	1.2352	13
over 100	3.4375	.9136	32

TABLE LXV

DESIGNATED SECURITY PERSON COMPARED TO SELECTED TOPICS

Response	Mean	Std Dev	Cases
	Topic B - Company Computer Security Programs		
	3.9032	.9685	248
Yes	4.0240	.9711	125
No	3.7805	.9542	123
	Topic C - Embezzlement: Detection and Control		
	3.4960	1.0377	248
Yes	3.4560	1.0739	125
No	3.5366	1.0024	123
	Topic E - Program Error		
	3.5927	.9936	248
Yes	3.5440	1.0121	125
No	3.6423	.9762	123
	Topic F - Operator Error		
	3.5927	.9689	248
Yes	3.6080	.9911	125
No	3.5772	.9496	123
	Topic G - Programmer Fraud		
	3.7137	1.0234	248
Yes	3.7600	1.0349	125
No	3.6667	1.0136	123
	Topic H - Operator Fraud		
	3.6694	1.0395	248
Yes	3.7440	1.0310	125
No	3.5935	1.0468	123

TABLE LXV (Continued)

Response	Mean	Std Dev	Cases
	Topic J - Hardware Protection		
	3.9718	.9325	248
Yes	3.9920	.9114	125
No	3.9512	.9569	123
	Topic M - Insurance Against Loss		
	3.4073	1.1201	248
Yes	3.3680	1.0891	125
No	3.4472	1.1538	123
	Topic N - Cryptographic Techniques		
	2.7339	1.0347	248
Yes	2.7840	1.0285	125
No	2.6829	1.0427	123
	Topic O - Protection When Using Service Bureaus		
	3.4534	1.0461	247
Yes	3.4274	1.1274	124
No	3.4797	.9611	123
	Topic P - Time-Sharing Protections		
	3.7166	1.0518	247
Yes	3.6935	1.0908	124
No	3.7398	1.0149	123
	Topic Q - Protection and Privacy Considerations		
	3.7742	.9678	248
Yes	3.8480	.9509	125
No	3.6992	.9829	123
	Topic R - Security Software Packages		
	3.2163	.9783	245
Yes	3.3200	1.0519	125
No	3.1083	.8868	120

TABLE LXVI

NUMBER OF SECURITY PERSONS COMPARED TO SELECTED TOPICS

Population	Mean	Std Dev	Cases
	Topic B - Company Computer Security Programs		
	4.0240	.9373	125
1	3.9828	.9821	58
2	3.9512	.9206	41
3	4.0000	.7385	12
4	4.4444	.7265	9
5	5.0000	.0000	2
6	4.0000	.0000	1
7	3.5000	2.1213	2
	Topic C - Embezzlement: Detection and Control		
	3.4720	1.0517	125
1	3.3793	1.1367	58
2	3.4634	.9246	41
3	3.7500	.7538	12
4	3.7778	1.0929	9
5	4.0000	1.4142	2
6	1.0000	.0000	1
7	4.0000	1.4142	2
	Topic E - Program Error		
	3.5760	1.0101	125
1	3.5517	.9764	58
2	3.7073	1.1455	41
3	3.5833	.6686	12
4	3.3333	.8660	9
5	3.5000	.7071	2
6	2.0000	.0000	1
7	3.5000	2.1213	2

TABLE LXVI (Continued)

Population	Mean	Std Dev	Cases
	Topic F - Operator Error		
	3.7240	.9892	125
1	3.5172	.9596	58
2	3.9024	1.0441	41
3	3.6667	.6513	12
4	3.3333	.8660	9
5	3.0000	1.4142	2
6	2.0000	.0000	1
7	3.5000	2.1213	2
	Topic G - Programmer Fraud		
	3.7520	1.0133	125
1	3.6897	.9589	58
2	3.8293	1.1598	41
3	3.9167	.6686	12
4	3.5556	1.0138	9
5	3.5000	2.1213	2
6	3.0000	.0000	1
7	4.5000	.7071	2
	Topic H - Operator Fraud		
	3.7600	1.0032	125
1	3.5862	1.0093	58
2	3.9268	1.1043	41
3	3.9167	.6686	12
4	3.7778	.8333	9
5	4.0000	1.4142	2
6	3.0000	.0000	1
7	4.5000	.7071	2
	Topic I - Hardware Protection		
	3.9920	.9025	125
1	3.9483	.9629	58
2	4.0732	.8772	41
3	4.0000	.7385	12
4	4.0000	.7071	9
5	3.5000	2.1213	2
6	4.0000	.0000	1
7	4.0000	1.4142	2

TABLE LXVI (Continued)

Population	Mean	Std Dev	Cases
	Topic M - Insurance Against Loss		
	3.3600	1.0954	125
1	3.3966	1.0077	58
2	3.3659	1.1566	41
3	3.7500	1.1382	12
4	2.7778	1.0929	9
5	3.0000	1.4142	2
6	2.0000	.0000	1
7	3.5000	2.1213	2
	Topic N - Cryptographic Techniques		
	2.8160	1.0348	125
1	2.8448	1.0226	58
2	2.7561	1.1786	41
3	2.9167	.6686	12
4	2.8889	.6009	9
5	2.5000	2.7071	2
6	1.0000	.0000	1
7	3.5000	2.1213	2
	Topic O - Protections When Using Service Bureaus		
	3.4480	1.1177	125
1	3.3793	1.2115	58
2	3.5366	1.0747	41
3	3.6667	.7785	12
4	3.3333	.7071	9
5	3.5000	2.1213	2
6	1.0000	.0000	1
7	4.0000	1.4142	2
	Topic P - Time-Sharing Protections		
	3.7177	1.0711	124
1	3.6316	1.1593	57
2	3.7805	1.0371	41
3	3.8333	.8348	12
4	3.8889	.7817	9
5	3.5000	2.1213	2
6	2.0000	.0000	1
7	4.5000	.7071	2

TABLE LXVI (Continued)

Population	Mean	Std Dev	Cases
Topic Q - Protection and Privacy Considerations			
	3.8320	.9733	125
1	3.7586	1.0141	58
2	3.8537	1.0139	41
3	3.9167	.9003	12
4	3.8889	.9280	9
5	4.0000	.0000	2
6	4.0000	.0000	1
7	4.5000	.7071	2
Topic R - Security Software Packages			
	3.3280	1.0455	125
1	3.1897	1.0338	58
2	3.3902	1.1375	41
3	3.6667	.7785	12
4	3.5556	.8819	9
5	3.5000	.7071	2
6	2.0000	.0000	1
7	3.5000	2.1213	2

APPENDIX H

MEANS OF ADDITIONAL COMPUTER

SECURITY TOPICS

TABLE LXVII

RESPONDENT'S PRESENT POSITION COMPARED TO SELECTED TOPICS

Value	Mean	Std Dev	Cases
Topic B - Company Computer Security Programs			
	3.9032	.9685	248
Data Processing Management	2.9066	.9844	182
Operational Management	3.8846	.9089	26
Security Analyst	3.5000	.7071	2
Other	3.9211	.9693	38
Topic C - Embezzlement: Detection and Control			
	3.4960	1.0377	248
Data Processing Management	3.5165	1.0654	182
Operational Management	3.4615	1.0288	26
Security Analyst	3.0000	.0000	2
Other	3.4474	.9500	38
Topic E - Program Error			
	3.5927	.9936	248
Data Processing Management	3.5714	1.0153	182
Operational Management	3.6438	.8458	26
Security Analyst	3.5000	.7071	2
Other	3.6579	1.0208	38
Topic F - Operator Error			
	3.5927	.9689	248
Data Processing Management	3.5824	1.0144	182
Operational Management	3.6154	.8038	26
Security Analyst	3.5000	.7071	2
Other	3.6316	.8829	38

TABLE LXVII (Continued)

Value	Mean	Std Dev	Cases
	Topic G - Programmer Fraud		
	3.7137	1.0234	248
Data Processing Management	3.6978	1.0678	182
Operational Management	3.7308	.9190	26
Security Analyst	3.0000	.0000	2
Other	3.8158	.8961	38
	Topic H - Operator Fraud		
	3.6694	1.0395	248
Data Processing Management	3.6758	1.0613	182
Operational Management	3.6154	.9829	26
Security Analyst	4.0000	1.4142	2
Other	3.6579	.9939	38
	Topic J - Hardware Protection		
	3.9718	.9325	248
Data Processing Management	3.9341	.9611	182
Operational Management	4.1154	.8162	26
Security Analyst	3.5000	.7071	2
Other	4.0789	.8817	38
	Topic M - Insurance Against Loss		
	3.4073	1.1201	248
Data Processing Management	3.3846	1.1348	182
Operational Management	3.8097	1.0590	26
Security Analyst	1.5000	.7071	2
Other	3.3421	.9939	38

TABLE LXVII (Continued)

Value	Mean	Std Dev	Cases
	Topic N - Cryptographic Techniques		
	2.7339	1.0347	248
Data Processing Management	2.6648	1.0043	182
Operational Management	3.0385	1.1826	26
Security Analyst	2.5000	.7071	2
Other	2.8684	1.0698	38
	Topic O - Protections When Using Service Bureaus		
	3.4534	1.0461	247
Data Processing Management	3.5165	1.0392	182
Operational Management	3.2800	1.1733	25
Security Analyst	3.5000	.7071	2
Other	3.2632	1.0050	38
	Topic P - Time-Sharing Protections		
	3.7166	1.0518	247
Data Processing Management	3.7348	1.0782	181
Operational Management	3.6538	1.0933	26
Security Analyst	3.5000	.7071	2
Other	3.6842	.9330	38
	Topic Q - Protection and Privacy Considerations		
	3.7742	.9678	248
Data Processing Management	3.8077	.9812	182
Operational Management	3.7308	1.0414	26
Security Analyst	4.0000	1.4142	2
Other	3.6316	.8517	38

TABLE LXVII (Continued)

Value	Mean	Std Dev	Cases
	Topic R - Security Software Packages		
	3.2163	.9783	245
Data Processing Management	3.1111	.9966	180
Operational Management	3.6538	.9774	26
Security Analyst	3.0000	.0000	2
Other	3.4324	.8007	37

TABLE LXVIII

RESPONDENT'S LENGTH OF TIME IN PRESENT POSITION
COMPARED TO SELECTED TOPICS

Value	Mean	Std Dev	Cases
Topic B - Company Computer Security Programs			
	3.9032	.9685	248
Less 1 year	3.6970	.8472	33
1-2 years	3.8529	1.2585	34
3-4 years	3.9351	.9225	77
5-6 years	4.1000	.8412	40
Over 6 years	3.8730	.9918	63
Topic C - Embezzlement: Detection and Control			
	3.4960	1.0377	248
Less 1 year	3.6970	.9838	33
1-2 years	3.1471	1.2585	34
3-4 years	3.5714	.9094	77
5-6 years	3.5250	1.0619	40
Over 6 years	3.4762	1.0604	63
Topic E - Program Error			
	3.5927	.9936	248
Less 1 year	3.6667	1.0206	33
1-2 years	3.3235	1.1990	34
3-4 years	3.4805	.9264	77
5-6 years	3.7250	.8767	40
Over 6 years	3.7619	.9954	63
Topic F - Operator Error			
	3.5927	.9689	248
Less 1 year	3.7879	.9273	33
1-2 years	3.4412	1.2356	34
3-4 years	3.4805	.8827	77
5-6 years	3.6750	.8590	40
Over 6 years	3.6667	1.0000	63

TABLE LXVIII (Continued)

Value	Mean	Std Dev	Cases
	Topic G - Programmer Fraud		
	3.7137	1.0234	248
Less 1 year	3.7879	.8200	33
1-2 years	3.5294	1.0220	34
3-4 years	3.6494	1.0484	77
5-6 years	4.0500	.9044	40
Over 6 years	3.6508	1.1382	63
	Topic H - Operator Fraud		
	3.6694	1.0395	248
Less 1 year	3.7273	.8758	33
1-2 years	3.4706	1.0220	34
3-4 years	3.6623	1.0464	77
5-6 years	4.0000	.8771	40
Over 6 years	3.5238	1.1758	63
	Topic J - Hardware Protection		
	3.9718	.9325	248
Less 1 year	3.8788	.9604	33
1-2 years	3.7353	.8981	34
3-4 years	4.0260	.9028	77
5-6 years	3.9500	.8756	40
Over 6 years	4.1111	1.0018	63
	Topic M - Insurance Against Loss		
	3.4073	1.1201	248
Less 1 year	3.1515	1.0642	33
1-2 years	3.3235	1.1735	34
3-4 years	3.5974	1.0792	77
5-6 years	3.4500	1.0610	40
Over 6 years	3.3651	1.1681	63

TABLE LXVIII (Continued)

Value	Mean	Std Dev	Cases
	Topic N - Cryptographic Techniques		
	2.7339	1.0347	248
Less 1 year	2.9394	1.0589	33
1-2 years	2.5294	1.2119	34
3-4 years	2.8701	.9645	77
5-6 years	2.7750	1.0497	40
Over 6 years	2.5556	.9801	63
	Topic O - Protections When Using Service Bureaus		
	3.4534	1.0461	247
Less 1 year	3.3333	.8898	33
1-2 years	3.0882	1.1901	34
3-4 years	3.5526	.9986	76
5-6 years	3.7750	1.0739	40
Over 6 years	3.3810	1.0384	63
	Topic P - Time-Sharing Protections		
	3.7166	1.0518	247
Less 1 year	3.6970	.8833	33
1-2 years	3.6176	1.1014	34
3-4 years	3.8182	1.0727	77
5-6 years	3.7949	1.0306	39
Over 6 years	3.6032	1.1150	63
	Topic Q - Protection and Privacy Considerations		
	3.7742	.9678	248
Less 1 year	3.7879	.8200	33
1-2 years	3.6176	1.0449	34
3-4 years	3.8052	.9602	77
5-6 years	3.9250	.9167	40
Over 6 years	3.6984	1.0416	63

TABLE LXVIII (Continued)

Value	Mean	Std Dev	Cases
	Topic R - Security Software Packages		
	3.2163	.9783	245
Less 1 year	3.2121	.9604	33
1-2 years	3.0303	1.1315	33
3-4 years	3.1867	.9683	75
5-6 years	3.3500	1.1447	40
Over 6 years	3.2698	.8074	63

TABLE LXIX

RESPONDENT'S LENGTH OF TIME IN COMPUTER-RELATED POSITION COMPARED TO SELECTED TOPICS

Value	Mean	Std Dev	Cases
	Topic B - Company Computer Security Programs		
	3.8984	.9799	246
Less 1 year	3.0000	.0000	1
1-2 years	5.0000	.0000	2
3-4 years	3.8571	1.2150	7
5-6 years	3.8462	.8006	13
7-10 years	3.7429	.7413	35
Over 10 years	3.9255	1.0105	188
	Topic C - Embezzlement: Detection and Control		
	3.5041	1.0371	246
Less 1 year	4.0000	.0000	1
1-2 years	5.0000	.0000	2
3-4 years	3.7143	.4880	7
5-6 years	3.6923	.9473	13
7-10 years	3.4571	.8859	35
Over 10 years	3.4734	1.0819	188
	Topic E - Program Error		
	3.5976	.9962	246
Less 1 year	2.0000	.0000	1
1-2 years	3.5000	.7071	2
3-4 years	4.0000	.8165	7
5-6 years	3.9231	.8623	13
7-10 years	3.6571	.9375	35
Over 10 years	3.5585	1.0195	188
	Topic F - Operator Error		
	3.5935	.9717	246
Less 1 year	2.0000	.0000	1
1-2 years	4.0000	1.4142	2
3-4 years	3.5714	.9759	7
5-6 years	3.8462	.9871	13
7-10 years	3.9143	.8869	35
Over 10 years	3.5213	.9727	188

TABLE LXIX (Continued)

Value	Mean	Std Dev	Cases
	Topic G - Programmer Fraud		
	3.7195	1.0255	246
Less 1 year	2.0000	.0000	1
1-2 years	5.0000	.0000	2
3-4 years	3.7143	.4880	7
5-6 years	3.4615	.8771	13
7-10 years	3.7714	.9103	35
Over 10 years	3.7234	1.0638	188
	Topic H - Operator Fraud		
	3.6667	1.0394	246
Less 1 year	2.0000	.0000	1
1-2 years	5.0000	.0000	2
3-4 years	3.8571	.6901	7
5-6 years	3.5385	.7763	13
7-10 years	3.8000	.9331	35
Over 10 years	3.6383	1.0782	188
	Topic J - Hardware Protection		
	3.9797	.9322	246
Less 1 year	4.0000	.0000	1
1-2 years	4.5000	.7071	2
3-4 years	4.2857	.9512	7
5-6 years	4.2308	1.0127	13
7-10 years	4.0000	.8745	35
Over 10 years	3.9415	.9432	188
	Topic M - Insurance Against Loss		
	3.4106	1.1094	246
Less 1 year	2.0000	.0000	1
1-2 years	3.5000	.7071	2
3-4 years	3.2857	.7559	7
5-6 years	3.9231	1.0377	13
7-10 years	3.2571	1.0387	35
Over 10 years	3.4149	1.1367	188

TABLE LXIX (Continued)

Value	Mean	Std Dev	Cases
	Topic N - Cryptographic Techniques		
	2.7439	1.0319	246
Less 1 year	2.0000	.0000	1
1-2 years	4.0000	.0000	2
3-4 years	2.8571	.8997	7
5-6 years	3.0769	1.1875	13
7-10 years	2.7429	.9500	35
Over 10 years	2.7074	1.0417	188
	Topic O - Protections When Using Service Bureaus		
	3.4612	1.0380	245
Less 1 year	3.0000	.0000	1
1-2 years	4.0000	.0000	2
3-4 years	2.8571	.8997	7
5-6 years	3.6923	.9473	13
7-10 years	3.0571	.9983	35
Over 10 years	3.5401	1.0433	187
	Topic P - Time-Sharing Protections		
	3.7265	1.0415	245
Less 1 year	3.0000	.0000	1
1-2 years	4.5000	.7071	2
3-4 years	3.7143	.9512	7
5-6 years	3.4615	1.0500	13
7-10 years	3.5143	1.0947	35
Over 10 years	3.7807	1.0370	187
	Topic Q - Protection and Privacy Considerations		
	3.7805	.9522	246
Less 1 year	4.0000	.0000	1
1-2 years	4.0000	.0000	2
3-4 years	4.0000	1.0000	7
5-6 years	3.4615	.6602	13
7-10 years	3.6857	.9000	35
Over 10 years	3.8085	.9841	188

TABLE LXIX (Continued)

Value	Mean	Std Dev	Cases
Topic R - Security Software Packages			
	3.2181	.9822	243
Less 1 year	5.0000	.0000	1
1-2 years	3.0000	1.4142	2
3-4 years	3.0000	1.4142	6
5-6 years	3.2500	.4523	12
7-10 years	3.1714	.9848	35
Over 10 years	3.2246	.9907	187

TABLE LXX

RESPONDENT'S HIGHEST EDUCATION LEVEL
COMPARED TO SELECTED TOPICS

Value	Mean	Std Dev	Cases
Topic B - Company Computer Security Programs			
	3.9065	.9707	246
High School Graduate	4.5556	.7265	9
Some College	3.7037	.9443	54
Associate Degree	3.8148	.7357	27
Vocational/Trade School Certificate	4.0833	.7930	12
Bachelor's Degree	3.8911	1.0668	101
Master's Degree	4.0714	.9472	42
Doctoral Degree	4.0000	.0000	1
Topic C - Embezzlement: Detection and Control			
	3.4959	1.0410	246
High School Graduate	3.7778	1.0929	9
Some College	3.4815	1.0594	54
Associate Degree	3.5556	.8916	27
Vocational/Trade School Certificate	4.2500	.8660	12
Bachelor's Degree	3.3762	1.0757	101
Master's Degree	3.4524	.9927	42
Doctoral Degree	5.0000	.0000	1
Topic E - Program Error			
	3.6016	.9917	246
High School Graduate	4.1111	.7817	9
Some College	3.7778	.9450	54
Associate Degree	3.5926	.8884	27
Vocational/Trade School Certificate	3.9167	.5149	12
Bachelor's Degree	3.5446	1.0726	101
Master's Degree	3.3333	1.0041	42
Doctoral Degree	3.0000	.0000	1

TABLE LXX (Continued)

Value	Mean	Std Dev	Cases
	Topic F - Operator Error		
	3.5935	.9633	246
High School Graduate	4.0000	.7071	9
Some College	3.7778	.9450	54
Associate Degree	3.4815	1.0141	27
Vocational/Trade School Certificate	3.8333	.5774	12
Bachelor's Degree	3.5347	1.0155	101
Master's Degree	3.4286	.9408	42
Doctoral Degree	3.0000	.0000	1
	Topic G - Programmer Fraud		
	3.7236	1.0206	246
High School Graduate	3.7778	1.3017	9
Some College	3.8333	.9857	54
Associate Degree	3.6667	1.0377	27
Vocational/Trade School Certificate	4.2500	.7538	12
Bachelor's Degree	3.6634	1.0225	101
Master's Degree	3.5952	1.0606	42
Doctoral Degree	4.0000	.0000	1
	Topic H - Operator Fraud		
	3.6789	1.0373	246
High School Graduate	3.5556	.8819	9
Some College	3.8148	.9727	54
Associate Degree	3.5926	1.1522	27
Vocational/Trade School Certificate	4.1667	.7177	12
Bachelor's Degree	3.6535	1.0811	101
Master's Degree	3.5000	1.0418	42
Doctoral Degree	4.0000	.0000	1

TABLE LXX (Continued)

Value	Mean	Std Dev	Cases
	Topic J - Hardware Protection		
	3.9715	.9363	246
High School Graduate	4.1111	.7817	9
Some College	4.0556	.8777	54
Associate Degree	4.1111	.8473	27
Vocational/Trade School Certificate	4.0833	1.1645	12
Bachelor's Degree	3.9010	1.0050	101
Master's Degree	3.8810	.8890	42
Doctoral Degree	4.0000	.0000	1
	Topic M - Insurance Against Loss		
	3.4146	1.1207	246
High School Graduate	4.0000	.8660	9
Some College	3.3889	1.0714	54
Associate Degree	3.5185	1.1887	27
Vocational/Trade School Certificate	4.1667	.7177	12
Bachelor's Degree	3.2178	1.1367	101
Master's Degree	3.5238	1.1527	42
Doctoral Degree	3.0000	.0000	1
	Topic N - Cryptographic Techniques		
	2.7398	1.0368	246
High School Graduate	2.8889	1.2693	9
Some College	2.7222	1.0888	54
Associate Degree	2.6667	.7845	27
Vocational/Trade School Certificate	3.0000	1.2060	12
Bachelor's Degree	2.7525	1.0431	101
Master's Degree	2.6429	1.0317	42
Doctoral Degree	4.0000	.0000	1

TABLE LXX (Continued)

Value	Mean	Std Dev	Cases
	Topic O - Protections When Using Service Bureaus		
	3.4612	1.0458	245
High School Graduate	3.8889	.7817	9
Some College	3.4074	1.0554	54
Associate Degree	3.5556	1.0860	27
Vocational/Trade School Certificate	3.5833	1.3114	12
Bachelor's Degree	3.5200	1.0394	100
Master's Degree	3.2143	1.0009	42
Doctoral Degree	3.0000	.0000	1
	Topic P - Time-Sharing Protections		
	3.7265	1.0494	245
High School Graduate	4.0000	1.1180	9
Some College	3.5926	1.0003	54
Associate Degree	3.8148	1.1448	27
Vocational/Trade School Certificate	3.8333	1.1934	12
Bachelor's Degree	3.8000	1.0445	100
Master's Degree	3.5476	1.0170	42
Doctoral Degree	5.0000	.0000	1
	Topic Q - Protection and Privacy Considerations		
	3.7724	.9715	246
High School Graduate	4.1111	.7817	9
Some College	3.6481	.9548	54
Associate Degree	3.7778	1.0500	27
Vocational/Trade School Certificate	3.9167	1.1645	12
Bachelor's Degree	3.7822	.9654	101
Master's Degree	3.7619	.9579	42
Doctoral Degree	5.0000	.0000	1

TABLE LXX (Continued)

Value	Mean	Std Dev	Cases
Topic R - Security Software Packages			
	3.2140	.9725	243
High School Graduate	4.0000	.7071	9
Some College	3.3269	1.0237	52
Associate Degree	2.9630	.8540	27
Vocational/Trade School Certificate	3.4167	1.3114	12
Bachelor's Degree	3.1100	.9309	100
Master's Degree	3.2381	.9579	42
Doctoral Degree	4.0000	.0000	1

APPENDIX I

MEANS OF ADDITIONAL COMPUTER SECURITY COURSES

TABLE LXXI

SELECTED COURSES IN CIS CURRICULUM COMPARED TO NUMBER OF PEOPLE EMPLOYED IN RESPONDENT'S COMPUTER CENTER (SECTION I-2 OF QUESTIONNAIRE)

Value	Mean	Std Dev	Cases
	CIS-1 Introduction to Computer-Based Systems		
	3.5344	1.1467	247
1-20	3.5500	1.1526	140
21-40	3.2162	1.2050	37
41-60	3.5500	1.0990	20
61-80	3.8333	.9832	6
81-100	3.8333	1.1146	12
Over 100	3.6563	1.1248	32
	CIS-2 Applications Program Development I		
	3.0766	1.0600	248
1-20	3.2143	1.0848	140
21-40	3.0541	1.0527	37
41-60	2.9500	.8870	20
61-80	3.3333	1.0328	6
81-100	2.6154	1.4456	13
Over 100	2.7188	.7719	32
	CIS-3 Applications Program Development II		
	3.4234	.9991	248
1-20	3.5214	1.0211	140
21-40	3.4054	.9267	37
41-60	3.2000	.8335	20
61-80	3.0000	.6325	6
81-100	3.0000	1.4720	13
Over 100	3.4063	.8747	32
	CIS-4 Systems Analysis Methods		
	3.8057	.9557	247
1-20	3.8849	.9409	139
21-40	3.7838	.9757	37
41-60	3.7000	.9787	20
61-80	3.5000	1.0488	6
81-100	3.5385	1.1983	13
Over 100	3.7188	.8884	32

TABLE LXXI (Continued)

Value	Mean	Std Dev	Cases
	CIS-5 Structured Systems Analysis and Design		
	3.7733	1.0227	247
1-20	3.7986	1.0369	139
21-40	3.8919	.8751	37
41-60	3.7500	1.0699	20
61-80	3.5000	1.3784	6
81-100	3.5385	1.1266	13
Over 100	3.6875	1.0298	32
	CIS-8 Software and Hardware Concepts		
	3.4531	.9511	245
1-20	3.4058	.9714	138
21-40	3.4722	.9407	36
41-60	3.2000	.8335	20
61-80	3.8333	.9832	6
81-100	3.8462	.6887	13
Over 100	3.5625	1.0140	32
	CIS-9 Office Automation		
	3.4268	1.0186	246
1-20	3.3381	1.0602	139
21-40	3.2778	1.0032	36
41-60	3.4500	.8870	20
61-80	3.5000	.5477	6
81-100	4.1538	.8987	13
Over 100	3.6563	.9370	32
	CIS-10 Decision Support Systems		
	3.4653	.9979	245
1-20	3.3957	1.0469	139
21-40	3.7143	.8935	35
41-60	3.5000	.8885	20
61-80	3.5000	1.0488	6
81-100	3.3846	.8697	13
Over 100	3.5000	1.0160	32

TABLE LXXI (Continued)

Value	Mean	Std Dev	Cases
	CIS-11 Advanced Database Concepts		
	3.8130	1.0130	245
1-20	3.8489	.9994	139
21-40	3.8889	1.0631	36
41-60	4.0000	1.0260	20
61-80	3.1667	.7528	6
81-100	3.6923	.9473	13
Over 100	3.6250	1.0701	32
	CIS-14 Information Systems Planning		
	3.7692	.9582	247
1-20	3.7842	.9613	139
21-40	3.9730	.9570	37
41-60	3.6500	.8751	20
61-80	3.3333	1.0328	6
81-100	3.6154	.9608	13
Over 100	3.6875	.9980	32

TABLE LXXII

SELECTED COURSES IN CIS CURRICULUM COMPARED TO PRESENCE OF DESIGNATED SECURITY PERSON IN RESPONDENT'S COMPUTER CENTER (SECTION I-3 OF QUESTIONNAIRE)

Value	Mean	Std Dev	Cases
	CIS-1 Introduction to Computer-Based Systems		
	3.5344	1.1467	247
Yes	3.5645	1.1351	124
No	3.5041	1.1621	123
	CIS-2 Application Program Development I		
	3.0766	1.0600	248
Yes	3.1280	1.0923	125
No	3.0244	1.0280	123
	CIS-3 Application Program Development II		
	3.4234	.991	248
Yes	3.4880	1.0672	125
No	3.3577	.9244	123
	CIS-4 Systems Analysis Methods		
	3.8057	.9557	247
Yes	3.8629	.9313	124
No	3.7480	.9801	123
	CIS-5 Structured Systems Analysis and Design		
	3.7733	1.0227	247
Yes	3.8306	1.0571	124
No	3.7154	.9878	123
	CIS-8 Software and Hardware Concepts		
	3.4531	.9511	245
Yes	3.5246	.9639	122
No	3.3821	.9367	123

TABLE LXXII (Continued)

Value	Mean	Std Dev	Cases
	CIS-9 Office Automation		
	3.4268	1.0186	246
Yes	3.4797	1.0191	123
No	3.3740	1.0195	123
	CIS-10 Decision Support Systems		
	3.4653	.9979	245
Yes	3.4309	1.0169	123
No	3.5000	.9812	122
	CIS-11 Advanced Database Concepts		
	3.8130	1.0130	246
Yes	3.8537	1.0611	123
No	3.7724	.9651	123
	CIS-14 Information Systems Planning		
	3.7692	.9582	247
Yes	3.7419	1.0191	124
No	3.7967	.8959	123

TABLE LXXIII

SELECTED COURSE IN CIS CURRICULUM COMPARED TO NUMBER OF DESIGNATED SECURITY PERSONS IN RESPONDENT'S COMPUTER CENTER (SECTION I-4 OF QUESTIONNAIRE)

Value	Mean	Std Dev	Cases
	CIS-1 Introduction to Computer-Based Systems		
	3.5403	1.1218	124
1	3.6034	1.2275	58
2	3.5250	.9334	50
3	3.6667	1.1547	12
4	3.2222	1.3017	9
5	2.5000	.7071	2
6	5.0000	.0000	1
7	3.0000	.0000	2
	CIS-2 Applications Program Development I		
	3.1200	1.0969	125
1	3.0862	1.0968	58
2	3.1951	1.1229	41
3	2.9167	1.2401	12
4	3.4444	1.0138	9
5	2.5000	.7071	2
6	2.0000	.0000	1
7	3.5000	.7071	2
	CIS-3 Applications Program Development II		
	3.4960	1.0748	125
1	3.3448	1.1479	58
2	3.6829	1.0354	41
3	3.5833	.9003	12
4	3.5556	1.0138	9
5	3.0000	.0000	2
6	2.0000	.0000	1
7	4.5000	.7071	2

TABLE LXXIII (Continued)

Value	Mean	Std Dev	Cases
	CIS-4 Systems Analysis Methods		
	3.8400	.9788	125
1	3.9138	.9603	58
2	3.7805	1.1071	41
3	3.7500	.7538	12
4	4.0000	.8660	9
5	3.0000	1.4142	2
6	3.0000	.0000	1
7	4.0000	.0000	2
	CIS-5 Structured Systems Analysis and Design		
	3.8480	1.0781	125
1	3.8276	1.1415	58
2	3.9268	1.0814	41
3	3.5833	.9962	12
4	3.8889	1.0541	9
5	4.0000	.0000	2
6	3.0000	.0000	1
7	4.5000	.7071	2
	CIS-8 Software and Hardware Concepts		
	3.4878	.9613	123
1	3.4561	1.0702	57
2	3.4634	.8396	41
3	3.5455	.8202	11
4	3.8889	.7817	9
5	2.5000	.7071	2
6	4.0000	.0000	1
7	3.5000	2.1213	2
	CIS-9 Office Automation		
	3.5081	1.0161	124
1	3.3684	.9934	57
2	3.4390	.9759	41
3	4.0000	1.2060	12
4	3.7778	1.0929	9
5	3.5000	.7071	2
6	4.0000	.0000	1
7	4.5000	.7071	2

TABLE LXXIII (Continued)

Value	Mean	Std Dev	Cases
	CIS-10 Decision Support Systems		
	3.4597	1.0073	124
1	3.4035	1.0498	57
2	3.5854	.9741	41
3	3.4167	.7930	12
4	3.5556	1.2360	9
5	2.5000	.7071	2
6	4.0000	.0000	1
7	3.0000	1.4142	2
	CIS-11 Advanced Database Concepts		
	3.8790	1.0327	124
1	3.9474	1.0423	57
2	3.8049	1.0775	41
3	3.5000	1.0000	12
4	4.0000	.8660	9
5	4.5000	.7071	2
6	3.0000	.0000	1
7	5.0000	.0000	2
	CIS-14 Information Systems Planning		
	3.7280	1.0110	125
1	3.7586	.9967	58
2	3.6829	1.0592	41
3	3.9167	1.0836	12
4	3.8889	.7817	9
5	3.0000	1.4142	2
6	2.0000	.0000	1
7	3.5000	.7071	2

TABLE LXXIV

SELECTED COURSES IN CIS CURRICULUM COMPARED
TO RESPONDENT'S PRESENT POSITION
(SECTION II-1 OF QUESTIONNAIRE)

Value	Mean	Std Dev	Cases
CIS-1 Introduction to Computer-Based Systems			
	3.5344	1.1467	247
Data Processing Management	3.5912	1.1493	181
Operational Management	3.4615	.9892	26
Security Analyst	4.5000	.7071	2
Other	3.2632	1.2233	38
CIS-2 Applications Program Development I			
	3.0766	1.0600	248
Data Processing Management	3.1209	1.0907	182
Operational Management	3.0769	.7442	26
Security Analyst	2.0000	1.4142	2
Other	2.9211	1.0751	38
CIS-3 Applications Program Development II			
	3.4234	.9991	248
Data Processing Management	3.4341	1.0478	182
Operational Management	3.3077	.6177	26
Security Analyst	4.5000	.7071	2
Other	3.3947	.9737	38
CIS-4 Systems Analysis Methods			
	3.8057	.9557	247
Data Processing Management	3.8729	.9192	181
Operational Management	3.6923	.9282	26
Security Analyst	1.5000	.7071	2
Other	3.6842	1.0162	38

TABLE LXXIV (Continued)

Value	Mean	Std Dev	Cases
CIS-5 Structured Systems Analysis and Design			
	3.7733	1.0227	247
Data Processing Management	3.8066	1.0172	181
Operational Management	3.7308	.8744	26
Security Analyst	3.0000	2.8284	2
Other	3.6842	1.0681	38
CIS-8 Software and Hardware Concepts			
	3.4531	.9511	245
Data Processing Management	3.4413	.9719	179
Operational Management	3.4615	.9892	26
Security Analyst	2.5000	.7071	2
Other	3.5526	.8285	38
CIS-9 Office Automation			
	3.4268	1.0186	246
Data Processing Management	3.4000	1.0496	180
Operational Management	3.5385	.8593	26
Security Analyst	4.0000	1.4142	2
Other	3.4474	.9781	38
CIS-10 Decision Support Systems			
	3.4653	.9979	245
Data Processing Management	3.4611	1.0214	180
Operational Management	3.4615	.9047	26
Security Analyst	3.5000	.7071	2
Other	3.4865	.9894	37

TABLE LXXIV (Continued)

Value	Mean	Std Dev	Cases
	CIS-11 Advanced Database Concepts		
	3.8130	1.0130	246
Data Processing Management	3.7722	1.0348	180
Operational Management	3.9231	.9767	26
Security Analyst	2.5000	2.1213	2
Other	4.000	.8383	38
	CIS-14 Information Systems Planning		
	3.7692	.9582	247
Data Processing Management	3.7680	.9839	181
Operational Management	3.6538	.9356	26
Security Analyst	4.0000	1.4142	2
Other	3.8421	.8551	38

TABLE LXXV

SELECTED COURSES IN CIS CURRICULUM COMPARED TO RESPONDENT'S LENGTH OF TIME AT PRESENT POSITION (SECTION II-2 OF QUESTIONNAIRE)

Value	Mean	Std Dev	Cases
CIS-1 Introduction to Computer-Based Systems			
	3.5344	1.1467	247
Less 1 year	3.4545	.9712	33
1-2 years	3.2647	1.2865	34
3-4 years	3.4545	1.1647	77
5-6 years	3.6154	.9898	39
Over 6 years	3.7460	1.2044	63
	5.0000	.0000	1
CIS-2 Applications Program Development I			
	3.0766	1.0600	248
Less 1 year	3.1212	.8200	33
1-2 years	2.8235	1.1670	34
3-4 years	3.1818	1.0604	77
5-6 years	3.1500	1.2100	40
Over 6 years	3.0476	.9907	63
	1.0000	.0000	1
CIS-3 Applications Program Development II			
	3.4234	.9991	248
Less 1 year	3.4242	.8671	33
1-2 years	3.1176	1.2001	34
3-4 years	3.5325	.8823	77
5-6 years	3.4000	1.1277	40
Over 6 years	3.4444	.9801	63
	5.0000	.0000	1
CIS-4 Systems Analysis Methods			
	3.8057	.9557	247
Less 1 year	3.7879	.8200	33
1-2 years	3.5000	1.1348	34
3-4 years	3.9481	.8255	77
5-6 years	3.9750	.9997	40
Over 6 years	3.7419	.9570	62
	1.0000	.0000	1

TABLE LXXV (Continued)

Value	Mean	Std Dev	Cases
CIS-5 Structured Systems Analysis and Design			
	3.7733	1.0227	247
Less 1 year	3.5758	1.2255	33
1-2 years	3.5294	1.1074	34
3-4 years	3.9221	1.0100	77
5-6 years	3.9000	.9554	40
Over 6 years	3.7258	.8902	62
	5.0000	.0000	1
CIS-8 Software and Hardware Concepts			
	3.4531	.9511	245
Less 1 year	3.4545	.7538	33
1-2 years	3.4412	1.0785	34
3-4 years	3.3947	1.0077	76
5-6 years	3.5500	.8458	40
Over 6 years	3.4754	.9934	61
	3.0000	.0000	1
CIS-9 Office Automation			
	3.4268	1.0186	246
Less 1 year	3.3939	.9663	33
1-2 years	3.2941	1.2193	34
3-4 years	3.3766	1.0265	77
5-6 years	3.4250	.9842	40
Over 6 years	3.5574	.9403	61
	5.0000	.0000	1
CIS-10 Decision Support Systems			
	3.4653	.9979	245
Less 1 year	3.5152	.9722	33
1-2 years	3.1515	1.1489	33
3-4 years	3.4156	1.0046	77
5-6 years	3.5500	1.0115	40
Over 6 years	3.6066	.8996	61
	4.0000	.0000	1

TABLE LXXV (Continued)

Value	Mean	Std Dev	Cases
	CIS-11 Advanced Database		
	3.8130	1.0130	246
Less 1 year	3.8435	.9722	33
1-2 years	3.6471	1.1776	34
3-4 years	3.8701	.9914	77
5-6 years	3.8250	1.0099	40
Over 6 years	3.8033	.9970	61
	4.0000	.0000	1
	CIS-14 Information Systems Planning		
	3.7692	.9582	247
Less 1 year	3.6061	.9334	33
1-2 years	3.7647	1.1297	34
3-4 years	3.7273	.9684	77
5-6 years	3.8750	.9658	40
Over 6 years	3.8226	.8594	62
	5.0000	.0000	1

TABLE LXXVI

SELECTED COURSES IN CIS CURRICULUM COMPARED TO RESPONDENT'S LENGTH OF TIME IN COMPUTER-RELATED POSITION (SECTION II-3 OF QUESTIONNAIRE)

Value	Mean	Std Dev	Cases
CIS-1 Introduction to Computer-Based Systems			
	3.5224	1.1436	245
Less 1 year	2.0000	.0000	1
1-2 years	4.0000	1.4142	2
3-4 years	3.4286	.9759	7
5-6 years	3.4615	1.1983	13
7-10 years	3.5588	.9906	34
Over 10 years	3.5266	1.1766	188
CIS-2 Applications Program Development I			
	3.0854	1.0560	246
Less 1 year	2.0000	.0000	1
1-2 years	2.5000	.7071	2
3-4 years	2.5714	.9759	7
5-6 years	2.9231	1.1152	13
7-10 years	3.1143	.8668	35
Over 10 years	3.1223	1.0900	188
CIS-3 Applications Program Development II			
	3.4187	.9977	246
Less 1 year	2.0000	.0000	1
1-2 years	2.0000	1.4142	2
3-4 years	3.7143	.7559	7
5-6 years	3.3077	1.1094	13
7-10 years	3.4000	.8812	35
Over 10 years	3.4415	1.0089	188
CIS-4 Systems Analysis Methods			
	3.8122	.9395	245
Less 1 year	3.0000	.0000	1
1-2 years	4.0000	.0000	2
3-4 years	3.5714	.5345	7
5-6 years	3.8462	1.2810	13
7-10 years	3.8286	.9231	35
Over 10 years	3.8182	.9385	187

TABLE LXXVI (Continued)

Value	Mean	Std Dev	Cases
	CIS-5 Structures Analysis Methods		
	3.7714	1.0227	245
Less 1 year	2.0000	.0000	1
1-2 years	4.0000	1.4142	2
3-4 years	4.2857	.7559	7
5-6 years	4.3077	.6304	13
7-10 years	3.8000	1.1061	35
Over 10 years	3.7166	1.0212	187
	CIS-8 Software and Hardware Concepts		
	3.4486	.9494	243
Less 1 year	4.0000	.0000	1
1-2 years	4.0000	1.4142	2
3-4 years	3.8571	.6901	7
5-6 years	3.6154	.6504	13
7-10 years	3.6857	.8668	35
Over 10 years	3.3676	.9808	185
	CIS-9 Office Automation		
	3.4139	1.0127	244
Less 1 year	2.0000	.0000	1
1-2 years	1.0000	.0000	2
3-4 years	3.2857	.7559	7
5-6 years	3.8462	.6887	13
7-10 years	3.5143	.8869	35
Over 10 years	3.4032	1.0313	186
	CIS-10 Decision Support Systems		
	3.4650	1.0009	243
Less 1 year	2.0000	.0000	1
1-2 years	1.0000	.0000	2
3-4 years	2.8571	.8997	7
5-6 years	3.6923	.9473	13
7-10 years	3.5429	.7005	35
Over 10 years	3.4919	1.0221	185

TABLE LXXVI (Continued)

Value	Mean	Std Dev	Cases
	CIS-11 Advanced Database Concepts		
	3.8074	1.0142	244
Less 1 year	3.0000	.0000	1
1-2 years	3.0000	2.8284	2
3-4 years	4.2857	.4880	7
5-6 years	3.8462	1.0682	13
7-10 years	3.4857	.9813	35
Over 10 years	3.8602	1.0037	186
	CS-14 Information Systems Planning		
	3.7592	.9556	245
Less 1 year	4.0000	.0000	1
1-2 years	3.5000	.7071	2
3-4 years	3.7143	.9512	7
5-6 years	3.8462	1.0682	13
7-10 years	3.8286	.8907	35
Over 10 years	3.7433	.9719	187

TABLE LXXVII

SELECTED COURSES IN CIS CURRICULUM COMPARED TO RESPONDENT'S HIGHEST EDUCATION LEVEL (SECTION II-4 OF QUESTIONNAIRE)

Value	Mean	Std Dev	Cases
CIS-1 Introduction to Computer-Based Systems			
	3.5407	1.1448	246
High School Graduate	3.7778	1.2019	9
Some College Work	3.3889	1.0714	54
Associate Degree	3.2963	1.1706	27
Vocational/Trade School Certificate	3.7500	.8660	12
Bachelor's Degree	3.6634	1.1600	101
Master's Degree	3.5000	1.2543	42
Doctoral Degree	3.0000	.0000	1
CIS-2 Application Program Development I			
	3.0894	1.0537	246
High School Graduate	3.3333	.8660	9
Some College Work	3.2222	.9842	54
Associate Degree	3.1481	.9488	27
Vocational/Trade School Certificate	3.6667	.9847	12
Bachelor's Degree	3.0099	1.0723	101
Master's Degree	2.8571	1.1806	42
Doctoral Degree	3.0000	.0000	1
CIS-3 Application Program Development II			
	3.4390	.9868	246
High School Graduate	3.5556	.7265	9
Some College Work	3.5000	.9467	54
Associate Degree	3.4444	.8006	27
Vocational/Trade School Certificate	3.9167	.9962	12
Bachelor's Degree	3.4158	.9926	101
Master's Degree	3.2619	1.1699	42
Doctoral Degree	3.0000	.0000	1

TABLE LXXVII (Continued)

Value	Mean	Std Dev	Cases
CIS-4 Systems Analysis Method			
	3.8082	.9581	245
High School Graduate	4.0000	.7071	9
Some College Work	3.7358	.9638	53
Associate Degree	3.9630	.8540	27
Vocational/Trade School Certificate	3.8333	.9374	12
Bachelor's Degree	3.8416	1.0172	101
Master's Degree	3.6667	.9542	42
Doctoral Degree	4.0000	.0000	1
CIS-5 Structured Systems Analysis and Design			
	3.7796	1.0205	245
High School Graduate	3.4444	.7265	9
Some College Work	3.6038	1.0623	53
Associate Degree	4.0370	.7586	27
Vocational/Trade School Certificate	3.6667	.9847	12
Bachelor's Degree	4.0099	1.0049	101
Master's Degree	3.3571	1.0551	42
Doctoral Degree	5.0000	.0000	1
CIS-8 Software and Hardware			
	3.4486	.9537	243
High School Graduate	3.6667	1.0000	9
Some College Work	3.4038	.9551	52
Associate Degree	3.4815	.9755	27
Vocational/Trade School Certificate	3.5000	.6742	12
Bachelor's Degree	3.4752	.9756	101
Master's Degree	3.3659	.9939	41
Doctoral Degree	3.0000	.0000	1

TABLE LXXVII (Continued)

Value	Mean	Std Dev	Cases
	CIS-9 Office Automation		
	3.4303	1.0180	244
High School Graduate	3.1111	1.6915	9
Some College Work	3.2885	.9359	52
Associate Degree	3.4444	.9740	27
Vocational/Trade School Certificate	3.7500	.8660	12
Bachelor's Degree	3.3861	.9692	101
Master's Degree	3.6667	1.1189	42
Doctoral Degree	4.0000	.0000	1
	CIS-10 Decision Support Systems		
	3.4691	.9969	243
High School Graduate	3.6667	1.1180	9
Some College Work	3.2885	1.0542	52
Associate Degree	3.5926	.9711	27
Vocational/Trade School Certificate	4.0000	.8528	12
Bachelor's Degree	3.4400	.9982	100
Master's Degree	3.4524	.9160	42
Doctoral Degree	5.0000	.0000	1
	CIS-11 Advanced Database Concepts		
	3.8156	1.0157	244
High School Graduate	3.7778	.9718	9
Some College Work	3.7692	1.1135	52
Associate Degree	3.8889	1.0500	27
Vocational/Trade School Certificate	4.0000	.7385	12
Bachelor's Degree	3.8614	.9902	101
Master's Degree	3.6667	1.0515	42
Doctoral Degree	4.0000	.0000	1

TABLE LXXVII (Continued)

Value	Mean	Std Dev	Cases
CIS-14 Information Systems Planning			
	3.7673	.9619	245
High School Graduate	3.8889	.6009	9
Some College Work	3.6981	.9320	53
Associate Degree	3.8148	.8787	27
Vocational/Trade School Certificate	3.8333	.8348	12
Bachelor's Degree	3.8218	1.0040	101
Master's Degree	3.6429	1.0780	42
Doctoral Degree	4.0000	.0000	1

APPENDIX J

CHI-SQUARE TESTS FOR SIGNIFICANCE

TABLE LXXVIII

COMPARISON OF WHETHER COMPUTER CENTER EMPLOYEES SHOULD POSSESS KNOWLEDGE OF COMPUTER SECURITY AND NUMBER OF EMPLOYEES IN RESPONDENT'S COMPUTER CENTER

Know-ledge	Number of Employees						Row Total
	1 - 20	21 - 40	41 - 60	61 - 80	81 - 100	Over 100	
Yes	141 56.9 82.5 48.6	37 14.9 92.5 12.8	20 8.1 83.3 6.9	6 2.4 85.7 2.1	13 5.2 100.0 4.5	31 12.5 88.6 10.7	248 85.5
No	30 71.4 17.5 10.3	3 7.1 7.5 1.0	4 9.5 16.7 1.4	1 2.4 14.3 .3		4 9.5 11.4 1.4	42 14.5
Column Total	171 59.0	40 13.8	24 8.3	7 2.4	13 4.5	35 12.1	290 100.0

P > .05 X^2 = 5.42634

P > .01 D.F. = 5

Significance = 0.3661

TABLE LXXIX

COMPARISON OF WHETHER COMPUTER CENTER EMPLOYEES SHOULD POSSESS KNOWLEDGE OF COMPUTER SECURITY AND PRESENCE OF SECURITY PERSON IN RESPONDENT'S COMPUTER CENTER

Knowledge	Security Person Yes	Security Person No	Row Total
Yes	125 50.4 88.7 43.1	123 49.6 82.6 42.4	248 85.5
No	16 38.1 11.3 5.5	26 61.9 17.4 9.0	42 14.5
	141 48.6	149 51.4	290 100.0

$P > .05$ $X^2 = 1.71322$

$P > .01$ D.F. = 1

Significance = 0.1906

TABLE LXXX

COMPARISON OF WHETHER COMPUTER CENTER EMPLOYEES SHOULD POSSESS KNOWLEDGE OF COMPUTER SECURITY AND NUMBER OF PEOPLE IN RESPONDENT'S COMPUTER CENTER DIRECTLY RESPONSIBLE FOR COMPUTER SECURITY

Knowl-edge	Number of People							Row Total
	1	2	3	4	5	6	7	
Yes	58	42	12	8	2	1	2	125
	46.4	33.6	9.6	6.4	1.6	.8	1.6	88.7
	90.6	87.5	85.7	88.9	100.0	100.0	66.7	
	41.1	29.8	8.5	5.7	1.4	.7	1.4	
No	6	6	2	1			1	16
	37.5	37.5	12.5	6.3			6.3	11.3
	9.4	12.5	14.3	11.1			33.3	
	4.3	4.3	1.4	.7			.7	
Column	64	48	14	9	2	1	3	141
Total	45.4	34.0	9.9	6.4	1.4	.7	2.1	100.0

P > .05 X^2 = 2.25705

P > .01 D.F. = 65

Significance = 0.8946

TABLE LXXXI

COMPARISON OF WHETHER COMPUTER CENTER EMPLOYEES SHOULD POSSESS KNOWLEDGE OF COMPUTER SECURITY AND RESPONDENT'S PRESENT POSITION

Knowl-edge	D. P. Management	Operational Management	Security Analyst	Other	Row Total
Yes	182	27	2	37	248
	73.4	10.9	.8	14.9	85.5
	85.4	93.1	100.0	80.4	
	62.8	9.3	.7	12.8	
No	31	2		9	42
	73.8	4.8		21.4	14.5
	14.6	6.9		19.6	
	10.7	.7		3.1	
Column Total	213	29	2	46	290
	73.4	10.0	.7	15.9	100.0

$P > .05$ $X^2 = 2.64653$

$P > .01$ D.F. = 3

Significance = 0.4494

TABLE LXXXII

COMPARISON OF WHETHER COMPUTER CENTER EMPLOYEES SHOULD POSSESS KNOWLEDGE OF COMPUTER SECURITY AND RESPONDENT'S LENGTH OF TIME IN PRESENT POSITION

Knowl-edge	Length of Time: Less 1 Year	1 - 2 Years	3 - 4 Years	5 - 6 Years	Over 6 Years	—	Row Total
Yes	33	34	77	40	63	1	248
	13.3	13.7	31.0	16.1	25.4	.4	85.5
	89.2	79.1	86.5	93.0	81.8	100.0	
	11.4	11.7	26.6	13.8	21.7	.3	
No	4	9	12	3	14		42
	9.5	21.4	28.6	7.1	33.3		14.5
	10.8	20.9	13.5	7.0	18.2		
	1.4	3.1	4.1	1.0	4.8		
Column Total	37	43	89	43	77	1	290
	12.8	14.8	30.7	14.8	26.6	.3	100.0

$P > .05$ $X^2 = 4.89396$

$P > .01$ D.F. = 5

Significance = 0.4290

TABLE LXXXIII

COMPARISON OF WHETHER COMPUTER CENTER EMPLOYEES SHOULD POSSESS KNOWLEDGE OF COMPUTER SECURITY AND RESPONDENT'S HIGHEST EDUCATIONAL LEVEL

Know-ledge	Educational Level							Row Total
	H.S. Grad	Some College	A.A.	Vo-Tech	B.A	M.A.	Ph.D.	
Yes	9	54	27	12	100	43	1	246
	3.7	22.0	11.0	4.9	40.7	17.5	.4	85.4
	69.2	84.4	84.4	75.0	89.3	87.8	50.0	
	3.1	18.8	9.4	4.2	34.7	14.9	.3	
No	4	10	5	4	12	6	1	42
	9.5	23.8	11.9	9.5	28.6	14.3	2.4	14.6
	30.8	15.6	15.6	25.0	10.7	12.2	50.0	
	1.4	3.5	1.7	1.4	4.2	2.1	.3	
Column Total	13	64	32	16	112	49	2	288
	4.5	22.2	11.1	5.6	38.9	17.0	.7	100.0

$P > .05$ $X^2 = 7.78645$

$P > .01$ D.F. = 6

Significance = 0.2542

TABLE LXXXIV

COMPARISON OF WHETHER COMPUTER CENTER EMPLOYEES SHOULD POSSESS KNOWLEDGE OF COMPUTER SECURITY AND RESPONDENT'S MAJOR AREA OF STUDY

Knowledge	Major: Comp. SC	Business	Engineering	Math	Arts & Science	Accounting	Other	Row Total
Yes	56	84	16	22	21	20	9	228
	24.6	36.8	7.0	9.6	9.2	8.8	3.9	86.4
	83.6	90.3	94.1	88.0	80.8	83.3	75.0	
	21.2	31.8	6.1	8.3	8.0	7.6	3.4	
No	11	9	1	3	5	4	3	36
	30.6	25.0	2.8	8.3	13.9	11.1	8.3	13.6
	16.4	9.7	5.9	12.0	19.2	16.7	25.0	
	4.2	3.4	.4	1.1	1.9	1.5	1.1	
Column Total	67	93	17	25	26	24	12	264
	25.4	35.2	6.4	9.5	9.8	9.1	4.5	100.0

$P > .05 \quad X^2 = 4.79649$

$P > .01 \quad D.F. = 6$

Significance = 0.5702

TABLE LXXXV

COMPARISON OF WHETHER COMPUTER CENTER EMPLOYEES SHOULD POSSESS KNOWLEDGE OF COMPUTER SECURITY AND NUMBER OF EMPLOYEES DIRECTLY SUPERVISED BY RESPONDENT

Knowl-edge	Number of Employees Supervised							Row Total
	None	1-5	6-10	11-15	16-20	21-25	Over 25	
Yes	19 7.7 79.2 6.6	97 39.1 85.8 33.4	45 18.1 81.8 15.5	34 13.7 89.5 11.7	15 6.0 83.3 5.2	8 3.2 100.0 2.8	30 12.1 88.2 10.3	248 85.5
No	5 11.9 20.8 1.7	16 38.1 14.2 5.5	10 23.8 18.2 3.4	4 9.5 10.5 1.4	3 7.1 16.7 1.0		4 9.5 11.8 1.4	42 14.5
Column Total	24 8.3	113 39.0	55 19.0	38 13.1	18 6.2	8 2.8	34 11.7	290 100.0

$P > .05$ $X^2 = 3.50592$

$P > .01$ D.F. = 6

Significance = 0.7432

TABLE LXXXVI

COMPARISON OF WHETHER COMPUTER CENTER EMPLOYEES SHOULD POSSESS KNOWLEDGE OF COMPUTER SECURITY AND RESPONDENT'S MEMBERSHIPS IN DATA PROCESSING PROFESSIONAL ORGANIZATIONS

Knowl-edge	Organizations				Row Total
	DPMA	ACM	DS Institute	Other	
Yes	237 98.8 85.3 84.0	1 .4 100.0 .4	1 .4 100.0 .4	1 .4 50.0 .4	240 85.1
No	41 97.6 14.7 14.5			1 2.4 50.0 .4	42 14.9
Column Total	278 98.6	1 .4	1 .4	2 .7	282 100.0

P > .05 $X^2 = 2.29928$

P > .01 D.F. = 3

Significance = 0.5127

TABLE LXXXVII

COMPARISON OF METHODS RESPONDENTS FELT WOULD BEST DEVELOP COMPUTER SECURITY KNOWLEDGE AND NUMBER OF EMPLOYEES IN RESPONDENTS COMPUTER CENTER

Develop Knowl-edge	Number of Employees 1 - 20	21 - 40	41 - 60	61 - 80	81 - 100	Over 100	Row Total
Sec. Course & Inc.	60 53.1 42.9 24.6	18 15.9 52.9 7.4	10 8.8 52.6 4.1	4 3.5 66.7 1.6	7 6.2 53.8 2.9	14 12.4 43.8 5.7	113 46.3
Sec. Course Only	110 55.0 7.9 4.5	6 30.0 17.6 2.5	2 10.0 10.5 .8			1 5.0 3.1 .4	20 8.2
Inc. Only	68 63.0 48.6 27.9	10 9.3 29.4 4.1	6 5.6 31.6 2.5	2 1.9 33.3 .8	5 4.6 38.5 2.0	17 15.7 53.1 7.0	108 44.3
Other	1 33.3 .7 .4		1 33.3 5.3 .4		1 33.3 7.7 .4		3 1.2
Column Total	140 57.4	34 13.9	19 7.8	6 2.5	13 5.3	32 13.1	244 100.0

$P > .05$ $X^2 = 19.91897$

$P > .01$ D.F. = 15

Significance = 0.1751

TABLE LXXXVIII

COMPARISON OF METHODS RESPONDENTS FEEL WOULD BEST DEVELOP COMPUTER SECURITY KNOWLEDGE AND WHETHER RESPONDENT'S COMPUTER CENTER HAS A DESIGNATED PERSON DIRECTLY RESPONSIBLE FOR COMPUTER SECURITY

Develop Knowledge	Security Person		Row Total
	Yes	No	
Sec. Course & Inc.	58 51.3 47.2 23.8	55 48.7 45.5 22.5	113 46.3
Sec. Course Only	9 45.0 7.3 3.7	11 55.0 9.1 4.5	20 8.2
Inc. Only	54 50.0 43.9 22.1	54 50.0 44.6 22.1	108 44.3
Other	2 66.7 1.6 .8	1 33.3 .8 .4	3 1.2
Column Total	123 50.4	121 49.6	244 100.0

$P > .05$ $X^2 = 0.59663$

$P > .01$ D.F. = 3

Significance = 0.8972

TABLE LXXXIX

COMPARISON OF METHODS RESPONDENTS FEEL WOULD BEST DEVELOP COMPUTER SECURITY KNOWLEDGE AND THE NUMBER OF PEOPLE IN RESPONDENT'S COMPUTER CENTER DIRECTLY RESPONSIBLE FOR COMPUTER SECURITY

Develop Knowl-edge	Number of People 1 - 20	21 - 40	41 - 60	61 - 80	81 - 100	Over 100	Row Total
Sec. Course & Inc.	21 35.6 36.8 17.1	26 44.1 65.0 21.1	5 8.5 41.7 4.1	5 8.5 55.6 4.1	1 1.7 50.0 .8		59 48.0
Sec. Course Only	4 40.0 7.0 3.3	3 30.0 7.5 2.4	2 20.0 16.7 1.6	1 10.0 11.1 .8			10 8.1
Inc. Only	31 59.6 54.4 25.2	10 19.2 25.0 8.1	5 9.6 41.7 4.1	3 5.8 33.3 2.4	1 1.9 50.0 .8	1 1.9 100.0 .8	52 42.3
Other	1 50.0 1.8 .8	1 50.0 2.5 .8					2 1.6
Column Total	57 46.3	40 32.5	12 9.8	9 7.3	2 1.6	1 .8	123 100.0

$P > .05$ $X^2 = 12.70079$

$P > .01$ D.F. = 18

Significance = 0.8090

TABLE LXXXX

COMPARISON OF METHODS RESPONDENTS FEEL WOULD BEST DEVELOP COMPUTER SECURITY KNOWLEDGE AND THE RESPONDENT'S PRESENT POSITION

Develop Knowl-edge	Number of Employees				Row Total
	Dp Mgmt	Op Mgmt	Sec Analyst	Other	
Sec. Course & Inc.	81 71.7 45.5 33.2	13 11.5 50.0 5.3	2 1.8 100.0 .8	17 15.0 44.7 7.0	113 46.3
Sec. Course Only	13 65.0 7.3 5.3	1 5.0 3.8 .4		6 30.0 15.8 2.5	20 8.2
Inc. Only	82 75.9 46.1 33.6	11 10.2 42.3 4.5		15 13.9 39.5 6.1	108 44.3
Other	2 66.7 1.1 .8	1 33.3 3.8 .4			3 1.2
Column Total	178 73.0	26 10.7	2 .8	38 15.6	244 100.0

$P > .05$ $X^2 = 8.16828$

$P > .01$ D.F. = 9

Significance = 0.5173

TABLE LXXXXI

COMPARISON OF METHODS RESPONDENTS FEEL WOULD BEST DEVELOP COMPUTER SECURITY KNOWLEDGE AND THE RESPONDENT'S LENGTH OF TIME IN PRESENT POSITION

Develop Know- ledge	Length of Time						Row Total
	Less 1	1-2 yrs	3-4 yrs	5-6 yrs	Over 6		
Sec.	18	13	42	17	22	1	113
Course	15.9	11.5	37.2	15.0	19.5	.9	46.3
& Inc.	56.3	38.2	55.3	42.5	36.1	100.0	
	7.4	5.3	17.2	7.0	9.0	.4	
Sec.	2	2	7	5	4		
Course	10.0	10.0	35.0	25.0	20.0		20
Only	6.3	5.9	9.2	12.5	6.6		8.2
	.8	.8	2.9	2.0	1.6		
Inc.	12	18	26	17	35		108
Only	11.1	16.7	24.1	15.7	32.4		44.3
	37.5	52.9	34.2	42.5	57.4		
	4.9	7.4	10.7	7.0	14.3		
Other		1	1	1			3
		33.3	33.3	33.3			1.2
		2.9	1.3	2.5			
		.4	.4	.4			
Column	32	34	76	40	61	1	244
Total	13.1	13.9	31.1	16.4	25.0	.4	100.0

P > .05 X^2 = 14.23887

P > .01 D.F. = 15

Significance = 0.5075

TABLE LXXXXII

COMPARISON OF METHODS RESPONDENTS FEEL WOULD BEST DEVELOP COMPUTER SECURITY KNOWLEDGE AND THE RESPONDENT'S LENGTH OF TIME IN A COMPUTER-RELATED POSITION

Develop Knowl-edge	Length of Time						Row Total
	Less 1	1-2 yrs	3-4 yrs	5-6 yrs	7-10 yrs	Over 10	
Sec. Course & Inc.	1 .9 100.0 .4		6 5.4 85.7 2.5	6 5.4 46.2 2.5	19 17.1 55.9 7.9	79 71.2 42.7 32.6	113 45.9
Sec. Course Only		1 5.0 50.0 .4		1 5.0 7.7 .4		18 90.0 9.7 7.4	20 8.3
Inc. Only		1 .9 50.0 .4	1 .9 14.3 .4	6 5.6 46.2 2.5	13 12.0 38.2 5.4	87 80.6 47.0 36.0	108 44.6
Other					2 66.7 5.9 .8	1 33.3 .5 .4	3 1.2
Column Total	1 .4	2 .8	7 2.9	13 5.4	34 14.0	185 76.4	242 100.0

P > .05 X^2 = 22.68534

P > .01 D.F. = 15

Significance = 0.0911

TABLE LXXXXIII

COMPARISON OF METHODS RESPONDENTS FEEL WOULD BEST DEVELOP COMPUTER SECURITY KNOWLEDGE AND THE RESPONDENT'S HIGHEST EDUCATIONAL LEVEL

Develop Knowl-edge	Educational Level							Row Total
	HS Grad	Some College	A.A.	Vo-Tech	B.A.	M.A.	Ph.D.	
Sec. Course & Inc.	4 3.6 44.4 1.7	23 20.5 43.4 9.5	10 8.9 37.0 4.1	7 6.3 70.0 2.9	50 44.6 50.0 20.7	18 16.1 42.9 7.4		112 46.3
Sec. Course Only		7 35.0 13.2 2.9	3 15.0 11.1 1.2	1 5.0 10.0 .4	6 30.0 6.0 2.5	3 15.0 7.1 1.2		20 8.3
Inc. Only	5 4.6 55.6 2.1	23 21.3 43.4 9.5	14 13.0 51.9 5.8	2 1.9 20.0 .8	43 39.8 43.0 17.8	20 18.5 47.6 8.3	1 .9 100.0 .4	108 44.6
Other					1 50.0 1.0 .4	1 50.0 2.4 .4		2 .8
Column Total	9 3.7	53 21.9	27 11.2	10 4.1	100 41.3	42 17.4	1 .4	242 100.0

$P > .05$ $X^2 = 10.91819$

$P > .01$ D.F. = 18

Significance = 0.8978

TABLE LXXXXIV

COMPARISON OF METHODS RESPONDENTS FEEL WOULD BEST DEVELOP COMPUTER SECURITY KNOWLEDGE AND THE RESPONDENT'S MAJOR AREA OF STUDY

Develop Knowl-edge	Major							Row Total
	Computer Science	Business	Engineer-ing	Math	Arts & Sci.	Account-ing	Other	
Sec. Course & Inc.	23 22.5 43.4 10.3	40 39.2 47.6 17.9	6 5.9 37.5 2.7	13 12.7 59.1 5.8	7 6.9 35.0 3.1	10 9.8 50.0 4.5	3 2.9 33.3 1.3	102 45.5
Sec. Course Only	2 10.5 3.8 .9	8 42.1 9.5 3.6	2 10.5 12.5 .9	1 5.3 4.5 .4	4 21.1 20.0 1.8	1 5.3 5.0 .4	1 5.3 11.1 .4	19 8.5
Inc. Only	27 27.0 50.9 12.1	34 34.0 40.5 15.2	8 8.0 50.0 3.6	8 8.0 36.4 3.6	9 9.0 45.0 4.0	9 9.0 45.0 4.0	5 5.0 55.6 2.2	100 44.6
Other	1 33.3 1.9 .4	2 66.7 2.4 .9						3 1.3
Column Total	53 23.7	84 37.5	16 7.1	22 9.8	20 8.9	20 8.9	9 4.0	224 100.0

$P > .05$ $X^2 = 11.24798$

$P > .01$ D.F. = 18

Significance = 0.8835

TABLE LXXXXV

COMPARISON OF METHODS RESPONDENTS FEEL WOULD BEST DEVELOP COMPUTER SECURITY KNOWLEDGE AND THE RESPONDENT'S EDUCATION OR TRAINING IN COMPUTER SECURITY

Develop Knowl-edge	College Courses	In-House Training	Seminars	Self-Edu.	No Training	Row Total
Sec. Course & Inc.	12 10.7 52.2 4.9	19 17.0 51.4 7.8	30 26.8 44.1 12.3	32 28.6 42.1 13.2	19 17.0 48.7 7.8	112 46.1
Sec. Course Only	2 10.0 8.7 .8	3 15.0 8.1 1.2	5 25.0 7.4 2.1	8 40.0 10.5 3.3	2 10.0 5.1 .8	20 8.2
Inc. Only	8 7.4 34.8 3.3	15 13.9 40.5 6.2	33 30.6 48.5 13.6	34 31.5 44.7 14.0	18 16.7 46.2 7.4	108 44.4
Other	1 33.3 4.3 .4			2 66.7 2.6 .8		3 1.2
Column Total	23 9.5	37 15.2	68 28.0	76 31.3	39 16.0	243 100.0

$P > .05$ $X^2 = 7.47495$

$P > .01$ D.F. = 12

Significance = 0.8247

TABLE LXXXXVI

COMPARISON OF METHODS RESPONDENTS FEEL WOULD BEST DEVELOP COMPUTER SECURITY KNOWLEDGE AND THE NUMBER OF EMPLOYEES DIRECTLY SUPERVISED BY THE RESPONDENT

Develop Knowledge	No. of Employees Supervised							Row Total
	None	1-5	6-10	11-15	16-20	21-25	Over 25	
Sec.	9	43	25	14	6	3	13	113
Course	8.0	38.1	22.1	12.4	5.3	2.7	11.5	46.3
& Inc.	47.4	45.3	54.3	42.4	40.0	42.9	44.8	
	3.7	17.6	10.2	5.7	2.5	1.2	5.3	
Sec.	2	8	5	1	2		2	20
Course	10.0	40.0	25.0	5.0	10.0		10.0	8.2
Only	10.5	8.4	10.9	3.0	13.3		6.9	
	.8	3.3	2.0	.4	.8		.8	
Inc.	8	43	16	18	7	4	12	108
Only	7.4	39.8	14.8	16.7	6.5	3.7	11.1	44.3
	42.1	45.3	34.8	54.5	46.7	57.1	41.4	
	3.3	17.6	6.6	7.4	2.9	1.6	4.9	
Other		1					2	3
		33.3					66.7	1.2
		1.1					6.9	
		.4					.8	
Column	19	95	46	33	15	7	29	244
Total	7.8	38.9	18.9	13.5	6.1	2.9	11.9	100.0

$P > .05$ $X^2 = 14.83545$

$P > .01$ D.F. = 18

Significance = 0.6732

TABLE LXXXXVII

COMPARISON OF METHODS RESPONDENTS FEEL WOULD BEST DEVELOP COMPUTER SECURITY KNOWLEDGE AND RESPONDENT'S MEMBERSHIP IN DATA PROCESSING PROFESSIONAL ORGANIZATIONS

Develop Knowl-edge	DPMA	ACM	DS Institute	Other	Row Total
Sec. Course & Inc.	109 99.1 46.8 46.2		1 .9 100.0 .4		110 46.6
Sec. Course Only	19 100.0 8.2 8.1				19 8.1
Inc. Only	103 98.1 44.2 43.6	1 1.0 100.0 .4		1 1.0 100.0 .4	105 44.5
Other	2 100.0 .9 .8				2 .8
Column Total	233 98.7	1 .4	1 .4	1 .4	236 100.0

P > .05 $X^2 = 3.64986$

P > .01 D.F. = 9

Significance = 0.9329

TABLE LXXXXVIII

COMPARISON OF WHETHER COMPUTER CENTER EMPLOYEES SHOULD POSSESS SOME KNOWLEDGE AND METHODS TO BEST DEVELOP KNOWLEDGE

Develop Knowl- edge	Yes	No	Row Total
Sec. Course & Inc.	113 100.0 46.5 46.3		113 46.3
Sec. Course Only	20 100.0 8.2 8.2		20 8.2
Inc. Only	107 99.1 44.0 43.9	1 .9 100.0 .4	108 44.3
Other	3 100.0 1.2 1.2		3 1.2
Column Total			244 100.0

$P > .05$ $X^2 = 1.26444$

$P > .01$ D.F. = 3

Significance = 0.7376

VITA

Karen Anne Forcht

Candidate for the Degree of

Doctor of Education

Thesis: AN ANALYSIS OF THE OPINIONS OF DATA PROCESSING MANAGEMENT ASSOCIATION MEMBERS CONCERNING DATA SECURITY CURRICULA IN HIGHER EDUCATION INSTITUTIONS

Major Field: Business Education

Biographical:

Personal Data: Born in Findlay, Ohio, April 17, 1944, the daughter of John and Rhea Bishop.

Education: Graduated from Arlington High School, Arlington, Ohio, in May, 1962; received Bachelor of Science degree in Business Education from Bowling Green State University, Bowling Green, Ohio, in December, 1970; received Master of Science degree in Computer Science from East Texas State University, Commerce, Texas, in June, 1974; completed requirements for the Doctor of Education degree at Oklahoma State University, Stillwater, Oklahoma, in December, 1984.

Professional Experience: High School Business Education Teacher at Findlay High School, Findlay, Ohio, Benjamin Logan High School, Zanesfield, Ohio, Hardin-Northern High School, Dola, Ohio, 1967-1971; Contract instructor in various education agencies of the United States Government, Washington, D.C., 1971-1972, Department Supervisor and Security Administrator for South Bend Tri-Governmental Computer Center, South Bend, Indiana, 1974; Lecturer in the Business Education Department, Wichita State University, Wichita, Kansas, 1977-1981; President of consulting group in Wichita, Kansas, 1978-1982; Graduate Teaching Associate, Department of Administrative Services and Business Education, Oklahoma State University, Stillwater, Oklahoma, 1982-1984.

Professional Organizations: Delta Pi Epsilon, Beta Gamma Sigma, Oklahoma Educational Microcomputer Association, National Business Education Association, Society of Data Educators, Southwest Federation of Administrative Disciplines, Administrative Services Association, Faculty Member of Pi Omega Pi.