

2

# NAVAL POSTGRADUATE SCHOOL Monterey, California

AD-A257 449



THESIS

DTIC  
ELECTE  
NOV 23 1992  
S E D

**COMPUTER SECURITY CONCEPTS and ISSUES  
in the INFORMATION TECHNOLOGY  
MANAGEMENT (370) CURRICULUM**

by

Reginald Wayne Vaughn

September 1992

Thesis Co-Advisor:  
Thesis Co-Advisor:

Dr. Tung X. Bui  
Roger Stemp

Approved for public release; distribution is unlimited.

92

3

92-29906  
10480

## REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION <b>UNCLASSIFIED</b>		1b. RESTRICTIVE MARKINGS	
2a. SECURITY CLASSIFICATION AUTHORITY		3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution is unlimited	
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE			
4. PERFORMING ORGANIZATION REPORT NUMBER(S)		5. MONITORING ORGANIZATION REPORT NUMBER(S)	
6a. NAME OF PERFORMING ORGANIZATION Computer Technology Dept. Naval Postgraduate School	6b. OFFICE SYMBOL (if applicable) 37	7a. NAME OF MONITORING ORGANIZATION Naval Postgraduate School	
6c. ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000		7b. ADDRESS (City, State, and ZIP Code) Monterey, CA 93943-5000	
8a. NAME OF FUNDING/SPONSORING ORGANIZATION	8b. OFFICE SYMBOL (if applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER	
8c. ADDRESS (City, State, and ZIP Code)		10. SOURCE OF FUNDING NUMBERS	
		PROGRAM ELEMENT NO.	PROJECT NO.
		TASK NO.	WORK UNIT ACCESSION NO.
11. TITLE (Include Security Classification) <b>COMPUTER SECURITY CONCEPTS and ISSUES in the INFORMATION TECHNOLOGY MANAGEMENT</b>			
12. PERSONAL AUTHOR(S) Vaughn, Reginald Wayne			
13a. TYPE OF REPORT Master's Thesis	13b. TIME COVERED From 09/91 To 09/92	14. DATE OF REPORT (Year, Month, Day) September 1992	15. PAGE COUNT 104
16. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the United States Government.			
17. COSATI CODES		18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)	
FIELD	GROUP	SUB-GROUP	
19. ABSTRACT (Continue on reverse if necessary and identify by block number) DoD has become increasingly dependent upon storing its sensitive information in electronic form and has a deep concern for the integrity and privacy of this valuable information. In the recent aftermath of numerous electronic break-ins, the DoD continues to express anxiety over technically weak system administrators' inability to protect sensitive electronic information.  The solution to minimizing these electronic intrusions and bolstering computer security in DoD is to educate military officers and federal civilians in the methods of computer security. This can be accomplished by integrating concepts and problem solving techniques related to computer security into the Information Technology Management (370) Curriculum at the Naval Postgraduate School.			
20. DISTRIBUTION/AVAILABILITY OF ABSTRACT <input checked="" type="checkbox"/> UNCLASSIFIED/UNLIMITED <input type="checkbox"/> SAME AS RPT. <input type="checkbox"/> DTIC USERS		21. ABSTRACT SECURITY CLASSIFICATION <b>UNCLASSIFIED</b>	
22a. NAME OF RESPONSIBLE INDIVIDUAL Dr. Tung X. Bui and Roger Stemp		22b. TELEPHONE (Include Area Code) (408) 646-2174	22c. OFFICE SYMBOL AS/Bd and CS/Sp

[11] Continued: (370) Curriculum

Approved for public release; distribution is unlimited

**COMPUTER SECURITY CONCEPTS and ISSUES in the INFORMATION  
TECHNOLOGY MANAGEMENT (370) CURRICULUM**

by  
Reginald Wayne Vaughn  
Lieutenant, United States Navy  
B.S., Lamar University, 1983

Submitted in partial fulfillment of the  
requirements for the degree of

**MASTER OF SCIENCE IN INFORMATION SYSTEMS**

from the  
**NAVAL POSTGRADUATE SCHOOL**  
September 1992

Author:

*Reginald Wayne Vaughn*  
Reginald Wayne Vaughn

Approved By:

*Tung X. Bui*  
Dr. Tung X. Bui, Co-Advisor

*R. Stemp*  
Roger Stemp, Co-Advisor

*David R. Whipple*  
David R. Whipple, Chairman,  
Department of Administrative Sciences

Accession For	
NTIS CRA&I	<input checked="" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification .....	
By .....	
Distribution / .....	
Availability Codes	
Dist	Avail and/or Special
A-1	

**DTIC QUALITY INSPECTED 4**

## **ABSTRACT**

**DoD has become increasingly dependent upon storing its sensitive information in electronic form and has a deep concern for the integrity and privacy of this valuable information. In the recent aftermath of numerous electronic break-ins, the DoD continues to express anxiety over technically weak system administrators' inability to protect sensitive electronic information.**

**The solution to minimizing these electronic intrusions and bolstering computer security in DoD is to educate military officers and federal civilians in the methods of computer security. This can be accomplished by integrating concepts and problem solving techniques related to computer security into the Information Technology Management (370) Curriculum at the Naval Postgraduate School.**

# TABLE OF CONTENTS

I.	INTRODUCTION .....	1
A.	RATIONALE AND PURPOSE OF THESIS .....	1
B.	SUMMARY OF CONTENTS.....	3
II.	COMPUTER SECURITY AND DOD .....	5
A.	WHAT IS COMPUTER SECURITY?.....	5
B.	DOD'S INTEREST IN COMPUTER SECURITY .....	6
1.	1989 U.S. General Accounting Office Report .....	6
2.	1991 U.S. General Accounting Office Report .....	7
3.	Computer Security Climate .....	9
C.	THE NEED FOR COMPUTER SECURITY PROFESSIONALS .....	9
III.	CULTIVATING COMPUTER SECURITY IN DOD .....	10
A.	SECURITY RELATED LEGISLATION .....	10
1.	NTISSP 200 .....	10
2.	Computer Security Act of 1987 .....	13
B.	FORMAL COMPUTER SECURITY EDUCATION .....	13
IV.	ANALYTICAL METHODS .....	16
A.	LITERATURE REVIEW .....	16
B.	LOGICAL COURSE GROUPINGS.....	17
C.	INTERVIEWS WITH NPS FACULTY .....	18
D.	INTERVIEWS WITH DOD ADP MANAGERS .....	18
E.	COURSE ANALYSES .....	19
V.	SUMMARY OF FINDINGS .....	20
VI.	RECOMMENDATIONS .....	23
VII.	CONCLUSION .....	30
APPENDIX A	Information Systems Courses .....	31
APPENDIX B	Computer Science Courses .....	52

APPENDIX C	Electro-Optical and Communication Courses .....	73
LIST OF REFERENCES	.....	94
INITIAL DISTRIBUTION LIST	.....	96

## **I. INTRODUCTION**

### **A. RATIONALE AND PURPOSE OF THESIS**

In 1986, Cliff Stoll, an astronomer-turned-system administrator at Lawrence Berkeley Laboratory, attracted international attention by tracing a 75 cent computer system accounting error to a West German hacker stealing military documents and selling them to the KGB. Although the hacker was not a brilliant programmer, he was persistent. By exploiting security deficiencies in operating systems, lax password security, and poor system management, the hacker managed to attack over 450 computers attached to MILNET, successfully penetrating 30. The hacker persistently attacked computers located at military bases, defense contractors, and universities, searching files for keywords like KH-11, SDI, and NUCLEAR. [Ref. 1]

On the evening of November 2, 1988, Robert T. Morris, a Cornell graduate student unleashed a worm on the Internet. Within hours approximately 3,000 Sun and VAX workstations running variants of the Berkeley Standard Distribution 4.3 UNIX operating system fell victim to the worm. Although the worm, innocuous in the sense that it did not destroy files or alter information, did however propagate uncontrollably, overwhelming system resources. [Ref. 2]

Between April 1990 and May 1991, foreign hackers penetrated 34 Department of Defense (DoD) computers including one system that directly supported Operation Desert Shield / Storm. The hackers gained access to sensitive military computers by exploiting well known flaws in operating systems, weaknesses in the Trivial File Transfer Protocol (TFTP) and accounts with easily guessed passwords. [Ref. 3]



DoD has become increasingly dependent upon storing its "sensitive information" in electronic form and naturally there is a deep concern for the integrity and privacy of this valuable information. In the aftermath of numerous electronic intrusions, many questions have been raised regarding the lack of computer security and the abundance of computer system vulnerabilities.

**One predominate factor linked to these "electronic break-ins" is system administrators who are not formally educated in computer security.** Although highly publicized stories of "electronic break-ins", worms, and viruses have made some system administrators more security conscious, **awareness of the problem is not enough.** [Ref. 4]

The phenomenon of widespread electronic intrusion is very recent. It is made possible by the proliferation of personal computers and their connection to electronic networks. Although technically sophisticated, intrusions are always the acts of human beings. Intrusions can be controlled by a combination of technical safeguards -- a sort of network immune system -- and hygienic procedures for using computers. But they **cannot** be eliminated.

It would seem that some straightforward technological fixes would greatly reduce future threats. But technological fixes are not the final answer; they are valid only until someone launches a new kind of attack. [Ref. 5]

The solution to minimizing these electronic intrusions and bolstering computer security in DoD is to educate military officers and federal civilians in the methods of computer security. This can be accomplished by integrating concepts and problem solving techniques related to computer security into the Information Technology Management (370) Curriculum at the Naval Postgraduate School.

The following describes DoD's anxiety about system administrators' inability to safeguard electronic information, and proposes several cost efficient avenues to enhance the training of computer security in the Information Technology Management (370) Curriculum. This thesis will also serve as a computer security reference vehicle to facilitate faculty members in modifying their courses to encompass relevant security issues.

## **B. SUMMARY OF CONTENTS**

This thesis contains seven chapters and three appendices, the following is a summary of the contents:

**Chapter I** *Introduction* acquaints the reader with three highly publicized electronic break-ins and highlights DoD's anxiety about technically weak system administrators' inability to protect sensitive electronic information.

**Chapter II** *Computer Security and DoD* briefly describes what computer security is and what it entails. Introduces two U.S. Government Accounting Office (GAO) perceptions of system administrators, the current "local" computer security climate, and the need for computer security professionals.

**Chapter III** *Cultivating Computer Security in DoD* describes laws, acts, and technical publications that directly impact computer security within DoD. Proposes modifying an academic program at the Naval Postgraduate School to ameliorate DoD's computer security problems.

**Chapter IV** *Analysis Methods* describes the procedures and resources used in this thesis.

**Chapter V** *Summary of Findings* summarizes the thesis research findings and the strengths and weaknesses of the current 370 Curriculum.

**Chapter VI** *Recommendations* describes in detail seven recommendations for improving computer security.

**Chapter VII** *Conclusion; opinions.*

**Appendix A** *Information Systems Courses* reflects the comparison of IS courses with the (ISC)<sup>2</sup> information security certification format.

**Appendix B** *Computer Science Courses* reflects the comparison of CS courses with the (ISC)<sup>2</sup> information security certification format.

**Appendix C** *Electro-Optical and Communication Courses* reflects the comparison of EO and CM courses with the (ISC)<sup>2</sup> information security certification format.

**List of References** lists the sources of information used.

## II. COMPUTER SECURITY AND DOD

### A. WHAT IS COMPUTER SECURITY?

In the aftermath of numerous "electronic break-ins" to sensitive government computers, the DoD has become acutely aware of its computer security inadequacies. In light of these recent events one must ponder the question, what exactly is computer security and what does it entail?

Computer security is far more reaching than just protecting information systems from "electronic break-ins".

Computer security is concerned with identifying vulnerabilities in systems and in protecting against threats to those systems....many computer users still don't really understand what computer security is--and why it should be important to them. Computer security protects your computer and everything associated with it--your building, your terminals and printers, your cabling, and your disks and tapes. Most importantly, computer security protects the information you've stored in your system. That's why computer security is often called **information security**. [Ref. 6]

"Every computer system is vulnerable to attack". [Ref. 7] In order to protect this valuable information, first determine where the system is susceptible to intrusion, attack, or environmental danger. Once you have discovered the system's vulnerabilities, appropriate preventative measures can be taken. Typical areas of concern include:

- **Physical Vulnerabilities:** Your buildings, your computer site and the associated peripherals are vulnerable. One of the primary functions of physical security is to restrict unauthorized access to the computer site and provide protection from damage caused by natural disasters. "Physical security methods include old fashioned locks and keys, as well as more advanced technologies like smart cards and biometric devices." [Ref. 8]

- **Natural Disasters**, such as fire, floods, earthquakes, and other dangers due to natural forces can cause irreparable damage to computer equipment and even worse, a loss of valuable information. Although natural disasters are not preventable, steps can be taken to minimize the severity of the damage.
- **Software Vulnerabilities:** Worms, viruses, trapdoors, and even simple bugs can open the system to electronic intruders.
- **Human Vulnerabilities:** "The people who administer and use your computer system represent the greatest vulnerability of all. The security of your entire system is often in the hands of a systems administrator." If that administrator is not properly trained or is unable to safeguard valuable electronic information, the system could be exploited and subjected to electronic terrorism or vandalism. [Ref. 9]

## **B. DOD'S INTEREST IN COMPUTER SECURITY**

### **1. 1989 U.S. General Accounting Office Report**

DoD has become increasingly dependent upon storing its "sensitive information" in electronic form and naturally there is a deep concern for the integrity and privacy of this valuable information.

Network intruders--some would call themselves explorers or liberators--have found ways of using networks to dial into remote computers, browse through their contents, and work their way into other computers. They have become skilled at cracking the password protocols that guard computers and adept at tricking the operating systems into giving them superuser or system manager privileges. They have also created worm and virus programs that can carry out these actions unattended and replicate themselves endlessly--electronic surrogates that can prowl the network independent of their creators. As electronic networking spreads around the globe, making possible new international interactions and breaching barriers of language and time, so rise the risks of damage to valuable information and the anxiety over attack by intruders, worms, and viruses. [Ref. 10]

Representative Edward J. Markey, Chairman of the Subcommittee on Telecommunications and Finance (House Committee on Energy and Commerce), recognizing the devastating impact a **malicious** "Internet type" worm could have on DoD computers, asked the U.S. General Accounting Office (GAO) to conduct an intensive investigation focusing on DoD's inherent vulnerabilities regarding computer security. [Ref. 11]

Hackers have been accessing and continue to gain access to sensitive networked DoD computer systems by exploiting system weaknesses. **One of the most prevalent weaknesses mentioned in the 1989 GAO report was that host computer site system managers were technically weak and practiced poor security management techniques.** The report states:

Host computers are frequently administered by systems managers, typically site personnel engaged in their own research, who often serve as systems managers on a part-time basis.

A number of Internet users, as well as NCSC and Defense Communications Agency virus reports, stated that the technical abilities of systems managers vary widely, with many managers poorly equipped to deal with security issues, such as the Internet virus. For example, according to the NCSC report, many systems managers lacked the technical expertise to understand that a virus attacked their systems and had difficulty administering fixes. **The report recommended that standards be established and a training program begun to upgrade systems manager expertise.** [Ref. 12]

## **2. 1991 U.S. General Accounting Office Report**

On November 20, 1991 Jack L. Brock Jr., Director of Government Information and Financial Management Issues (Information Management and Technology Division) gave testimony before the members of the Senate

Subcommittee on the vulnerabilities of DoD computer systems penetrated during Operation Desert Shield / Storm. Mr. Brock stated:

Hackers continue to successfully exploit security weaknesses and undermine the integrity and confidentiality of sensitive government information.

Between April 1990 and May 1991, computer systems at 34 DoD sites attached to the Internet were successfully penetrated by foreign hackers. The hackers exploited well-known security weaknesses--many of which were exploited in the past by other hacker groups. These weaknesses persist because of the inadequate attention to computer security, such as password management, **and the lack of technical expertise on the part of some system administrators--persons responsible for the technical management of the system.**

At many of the sites the hackers had access to unclassified, sensitive information on such topics as (1) military personnel-- personnel performance reports, travel information and personnel reductions; (2) logistics--descriptions of the type and quantity of equipment being moved; and (3) weapons systems development data.

Although such information is unclassified, it can be highly sensitive, particularly during times of international conflict. Some DoD and government officials have expressed concern that the aggregation of unclassified, sensitive information could result in the compromise of classified information.

**...system administration duties are generally part-time duties and that administrators frequently have little computer security background or training. [Ref. 13]**

Both GAO reports express DoD's anxiety about system administrators' lack of technical expertise and their inability to safeguard electronic information.

### **3. Computer Security Climate**

To obtain a feel for the "local" computer security climate, interviews were conducted with the System Administrator/Automated Data Processing (ADP) Managers at two central California military installations to determine their computer security backgrounds and training. Research revealed that the system administrators received little if any formal education in the arena of computer security. For example, one of the ADP Manager's entire formal training consisted of a two day computer security course in San Francisco [Ref. 14]. The other ADP Manager had not received any type of formal computer security training to date [Ref. 15].

### **C. THE NEED FOR COMPUTER SECURITY PROFESSIONALS**

It is imperative that the concepts and issues of computer security be addressed if our goal is to protect the privacy, integrity and availability of sensitive government information from forms of electronic vandalism and terrorism. To accomplish this goal, attention must be focused on establishing an education program that will provide system administrators with the technical expertise to understand, administer, and make knowledgeable, informed decisions with regard to computer security.



### **III. CULTIVATING COMPUTER SECURITY IN DOD**

#### **A. SECURITY RELATED LEGISLATION**

Since the late 1950s, federal agencies have become increasingly concerned over the protection of sensitive electronic information. This concern has spawned numerous pieces of legislation aimed at security. Two recent pieces of legislation, the National Telecommunication and Information Systems Security Publication 200 (NTISSP 200) and the Computer Security Act of 1987, have had a profound impact on the delegation of computer security practices in DoD.

##### **1. NTISSP 200**

National Telecommunication and Information Systems Security Publication 200 (National Policy on Controlled Access Protection) defined a minimum level of protection for computer systems operated by Executive branch agencies and departments of the U.S. Government. The policy applies to any system accessed by multiple users who do not all have the same authorization to use all of the classified or sensitive unclassified information processed or maintained by the system. NTISSP 200 stated that within five years of publication (i.e., by September of 1992), the systems affected by the policy must provide automated Controlled Access Protection (CAP) for all classified and sensitive unclassified information at the C2 level of trust defined in the Orange Book.<sup>1</sup> [Ref. 16]

The Orange Book is a technical publication, part of the Rainbow Series<sup>2</sup>, which defines trusted computer system evaluation criteria for systems requiring multiple levels of security. There are four basic divisions of trust,

---

1. Department of Defense Trusted Computer System Evaluation Criteria, Department of Defense Standard (DOD 5200.28-STD) Library Number S225,711, December 1985.

2. A series of technical computer security books published by the National Computer Security Center, each with a different colored covering, hence the name "Rainbow Series"

with each division further subdivided into one or more distinct classes. Each class is denoted with a number, where the higher numbers indicate a greater degree of security [Ref. 17]. In increasing order of trust, from lowest to highest, the classes are:




- D Minimal Protection
- C1 Discretionary Security Protection
- C2 Controlled Access Protection
- B1 Labeled Security Protection
- B2 Structured Protection
- B3 Security Domains
- A1 Verified Design

How do you rate each of the aforementioned classes, and what are the associated requirements to achieve this rating?

Each class is defined by a specific set of criteria that a system must met to be awarded a rating for that class. The criteria fall into four general categories: **security policy**, **accountability**, **assurance**, and **documentation**. [Ref. 18] Table 1 compares the Orange Book evaluation classes, showing the specific features required for each class and, in general terms, how requirements increase from class to class. [Ref. 19]

**Table 1: TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA**

	C1	C2	B1	B2	B3	A1	
Discretionary Access Control							Security Policy
Object Reuse							
Labels							
Label Integrity							
Exploitation of Labeled Information							
Exploitation of Multilevel Devices							
Labeling Human-Readable Output							
Mandatory Access Control							
Subject Sensitivity Labels							
Device Labels							
Identification and Authentication							Accountability
Audit							
Trusted Path							
System Architecture							Assurance
System Integrity							
Security Testing							
Design Specification and Verification							
Covert Channel Analysis							
Trusted Facility Management							
Configuration Management							
Trusted Recovery							
Trusted Distribution							
Security Features User's Guide							Documentation
Trusted Facility Manual							
Test Documentation							
Design Documentation							

-  New or enhanced requirements for this class
-  No additional requirements for this class
-  No requirements for this class

## **2. Computer Security Act of 1987**

The Computer Security Act of 1987 holds each federal agency accountable for identifying computer systems that utilize sensitive data. The act also requires civilian, military, government employees, and others who directly interact with systems containing sensitive information to receive computer security training commensurate with their level of access. [Ref. 9]

Since the government has over 50,000 sensitive systems, a new stock of questions emerge. Who will train this multitude of individuals needed to operate these systems, to what extent will they be trained, and how will their computer security training benefit the DoD?

### **B. FORMAL COMPUTER SECURITY EDUCATION: TOWARD A CERTIFICATION FORMAT**

**System administrators are chronically considered the weak link in the computer security chain.** Their lack of formal and technical education in the arena of computer security is a dangerous situation, but this situation can be rectified.

The Naval Postgraduate School (NPS) in Monterey, California, an institution dedicated to providing graduate level academic programs to meet the increasing technological and professional needs of the DoD, offers a viable solution. The Information Technology Management (370) Curriculum, an eight quarter interdisciplinary program of study, is designed to provide officers and federally employed civilians with a strong knowledge of information systems, emphasizing computer and telecommunication systems.

With minor modifications and a moderate injection of computer security concepts and issues, the Information Technology Management (370)

Curriculum can become a beneficial vehicle for producing more knowledgeable and competent computer security "professionals". The modified curriculum can greatly contribute towards combating DoD's computer security problems.

There are individuals in the computer industry who market themselves as "security professionals", but without the sanction of any recognized certifying group. A few certification programs lightly touch on security issues, but to date, there is no certification program dedicated totally to the issues of information security. [Ref. 20]

The International Information Systems Security Certification Consortium-- or (ISC)<sup>2</sup> for short-- was created to develop a certification program for information systems security practitioners. In November 1988, the Special Interest Group for Computer Security (SIG-CS) of the Data Processing Management Association (DPMA) brought together organizations who were interested in creating a certification program for this community of specialists. The cooperating organizations include the Data Processing Management Association (DPMA), Information Systems Security Association (ISSA), Idaho State University, the National Security Agency (NSA), and the Computer Security Institute (CSI). Other groups --including the Canadian and U.S. Governments, the Canadian Information Processing Society (CIPS), and the International Federation for Information Processing (IFIO) have been represented at meetings and have been invited to participate. Representation from other interested and qualified bodies, including IEEE and ACM, is under consideration. [Ref. 21]

In 1991 (ISC)<sup>2</sup> proposed the first formal certification program for computer security professionals. This certification reflects the current thought and future expectations of distinguished experts in the computer security field. [Ref. 22]

By extracting the (ISC)<sup>2</sup> certification format and injecting these concepts and issues into the existing 370 Curriculum, a new, enhanced curriculum will metamorphose. **In this fast changing climate of high-technology, this curriculum will ensure the military has an ample supply of these top-level managers and supervisors who possess a solid background in the area of computer security.**

## IV. ANALYTICAL METHODS

The purpose of this thesis is to determine if relevant computer security concepts and issues were being addressed in the Information Technology Management (370) Curriculum and make recommendations to improve course content and the Curriculum. In order to determine which concepts and issues were considered relevant and if they were being addressed, several methods were employed:

- Literature review (including academic and DoD publications on computer security).
- Interviews with DoD ADP Managers.
- Interviews with faculty from the Computer Science, Administrative Sciences, and the Electrical and Computer Engineering Departments.
- Micro analysis of the 370 Curriculum from the viewpoint of computer security, utilizing the (ISC)<sup>2</sup> certification format.

### A. LITERATURE REVIEW

Initially, a comprehensive literature review was conducted to become familiar with the current computer security atmosphere and to form a knowledge base for further research. The computer library located in the Naval Postgraduate School's Ingersoll Hall, is a cornucopia of computer information. Some of the reference material utilized to assimilate information for the knowledge base includes;

- Government Publications: The "Rainbow Series", Federal Information Processing Standards Publications (FIPS PUBS) and Government Accounting Office Reports (GAO)
- Electronic Newsgroups: **alt.security, comp.risks, comp.virus**

- Anonymous File Transfer Protocol (FTP): Several documents were retrieved electronically from these addresses: [cert.sei.cmu.edu](http://cert.sei.cmu.edu), [cu.nih.gov](http://cu.nih.gov), [cs.purdue.edu](http://cs.purdue.edu).
- Computer Security Books: *Computers under Attack: Intruders, Worms and Viruses* by Peter Denning, *Security in Computing* by Charles Pfleeger, *Computer Security Basics* by Deborah Russell and G.T. Gangemi Sr., and *Computer Security Handbook* by Richard Baker.
- Computer Security Professional Certification Format: International Information Systems Security Certification Consortium (ISC)<sup>2</sup> is the format used to evaluate each course in the 370 Curriculum. The result of the evaluation is reflected in Appendices A, B, and C.

Once the information from the literature review was assimilated, and a through knowledge of computer security established. This newly gained knowledge base, along with the (ISC)<sup>2</sup> certification format was used as a tool to interview NPS faculty members.

## **B. LOGICAL COURSE GROUPINGS**

To analyze the 370 Curriculum, it was necessary to segregate the courses into the following logical course groupings; Communications (CM), Computer Science (CS), Electro-Optical (EO), Information Systems (IS), Management (MN), Operations Science (OS), Mathematics (MA), and Naval Science (NS). Research revealed the MN, OS, MA, and NS courses were sufficiently devoid of the information applicable to computer security. Four course groupings: IS, CS, CM and EO were selected for analysis because they contained the bulk of the technical material in the 370 Curriculum and relate to computer systems. Once the areas for analysis were selected, the experts were interviewed.



### C. INTERVIEWS WITH NPS FACULTY

Faculty members representing the Computer Science, Administrative Science, and the Electrical and Computer Engineering departments were individually interviewed. Each interview revolved around four main issues:

- To what extent did the course address computer security concepts and issues?
- If the concepts and issues were not addressed, how easy would it be to incorporate the (ISC)<sup>2</sup> format into the course?
- If the concepts and issues were addressed, how close did the content adhere to the (ISC)<sup>2</sup> format?
- If there were shortcomings in the amount of computer security issues addressed, where could improvements be made?

Each emphasis area course within its respective department was reviewed for computer security related concepts or issues. Faculty members were encouraged to offer their opinions as to how the courses could be modified to adhere to the (ISC)<sup>2</sup> certification format.

### D. INTERVIEWS WITH DOD ADP MANAGERS

Interviews were conducted with the System Administrator/Automated Data Processing (ADP) Managers at two central California military installations to determine their computer security backgrounds and training.

Interview questions focused on;

- **Personal Education:** Did the individual have any previous computer experience, if so what type, and how much?
- **Training:** What type of computer security training had they received? What actions were taken to increase the staff's awareness of computer security? What type of guidance did they receive (e.g. local instructions, Navy instructions, laws, etc...).

What were their future plans to increase computer security and computer security awareness at their site?

#### **E. COURSE ANALYSES**

Four logical course grouping areas of the 370 Curriculum; Information Systems, Computer Science, Communications and Electro-Optical were analyzed. Each course in the respective logical course grouping was scrutinized for relevant computer security issues using the (ISC)<sup>2</sup> certification format as a cross-reference. **Each course fell into one of three categories, either the subject was addressed, the subject was not addressed but needs to be, or the subject was not relevant to the course.**

## V. SUMMARY OF FINDINGS

Both the 1989 and 1991 GAO reports discussed in chapter 2, express DoD's anxiety about technically weak system administrator's inability to protect sensitive electronic information. Both reports recommend a formal training program be established to strengthen system administrator's knowledge of computer security.

Interviews with local ADP managers support the GAO's findings that system administrators receive little if any formal computer security training. Although only a small portion of the ADP manager population was sampled, it was evident that formal computer security training had not been a prerequisite for the position.

Faculty interviews along with course analyses indicate only one course, **CS 4601 Computer Security**, adheres closely to the (ISC)<sup>2</sup> certification format, and that computer security concepts and issues are sparse in other courses of the 370 Curriculum. Of the 298 topic items identified by the (ISC)<sup>2</sup> certification format, 165 items are addressed in CS 4601 Computer Security, 37 items are addressed in IS 4200 System Analysis and Design, 10 items are addressed in CM 3112 Navy Telecommunications Systems, and 6 items in CS 2970 Structured Programming with Ada. Those courses that actually addressed computer security concepts or issues are highlighted in the current 370 Curriculum matrix shown in Table 2.

**Table 2: CURRENT INFORMATION TECHNOLOGY MANAGEMENT (370)  
CURRICULUM**

<b>1 st Quarter</b>	<b>IS 2000 (3-1)</b> Introduction to Computer Management	<b>CS 2970 (4-1)</b> Structured Programming with Ada	<b>OS 3101 (4-1)</b> Statistical Analysis for Management	<b>MN 2155 (4-0)</b> Accounting for Management
<b>2 nd Quarter</b>	<b>CS 3030 (4-0)</b> Computer Architecture and Operating Systems	<b>MA 1248 (4-1)</b> Selected Topics in Applied Mathematics	<b>OS 3004 (5-0)</b> Operations Research for Computer Systems Managers	<b>MN 3105 (4-0)</b> Organization and Management
<b>3 rd Quarter</b>	<b>IS 4200 (4-0)</b> System Analysis and Design	<b>EO 2710 (4-2)</b> Comm Systems I: Analog Signals and Systems	<b>IS 4183 (4-1)</b> Applications of Database Management Systems	<b>IS 3170 (4-0)</b> Economic Evaluation of Information Systems I
<b>4 th Quarter</b>	<b>IS 3020 (3-2)</b> Software Design	<b>EO 2750 (4-2)</b> Comm Systems II: Digital Signals and Systems	<b>IS 4185 (4-1)</b> Decision Support Systems	<b>IS 3171 (4-0)</b> Economic Evaluation of Information Systems II
<b>5 th Quarter</b>	<b>IS 4300 (4-0)</b> Software Engineering and Management	<b>EO 3750 (4-0)</b> Communications System Analysis	<b>IS 3502 (4-0)</b> Computer Networks: Wide Area / Local Area	<b>CM 3112 (4-0)</b> Navy Telecommunications Systems
<b>6 th Quarter</b>	<b>MN 4125 (4-0)</b> Managing Planned Change in Complex Organizations	<b>NS 3252 (4-0)</b> Joint and Maritime Strategic Planning	<b>IS 4502 (4-0)</b> Telecommunications Networks	<b>IS 0810 (0-0)</b> Thesis Research for Information Technology Management Students
<b>7 th Quarter</b>	<b>MN 3154 (4-0)</b> Financial Management in the Armed Forces	<b>CS 4681 (4-0)</b> Computer Security	<b>MN 3307 (4-0)</b> ADP Acquisition	<b>IS 0810 (0-0)</b> Thesis Research for Information Technology Management Students
<b>8 th Quarter</b>	<b>IS 4182 (4-0)</b> Information Systems Management	<b>Elective</b>	<b>IS 0810 (0-0)</b> Thesis Research for Information Technology Management Students	<b>IS 0810 (0-0)</b> Thesis Research for Information Technology Management Students

For a detailed analysis of how well each course paralleled the relevant computer security concepts in (ISC)<sup>2</sup> certification format see the following appendices. [Ref. 20]

- APPENDIX A Information Systems Courses
- APPENDIX B Computer Science Courses
- APPENDIX C Electro-Optical and Communication Courses

In order to help decipher the appendices, a small sample is provided in Table 3.

**Table 3: APPENDIX LEGEND**

COMPUTER SECURITY CONCEPTS AND ISSUES	IS 2000	IS 3020	IS 3170	IS 3171	IS 3183	IS 3502	IS 4182	IS 4185	IS 4200	IS 4300	IS 4502
<b>I. Overview</b>											
<b>A. Development of a Security Program</b>											
1. Reason for a organizational security management policy											
a. Objectives											
1. Identify sensitive systems/data	+						+				
2. Security plan	+						+				
3. Training	+						+				



The concept or issue is currently addressed.



The concept or issue is not currently addressed, but needs to be.



The concept or issue is not relevant to the course.

## VI. RECOMMENDATIONS

Research indicates that the current 370 Curriculum needs a moderate injection of additional computer security topics to emulate the (ISC)<sup>2</sup> certification format. Several recommendations for modifying the 370 Curriculum follow:

**Recommendation 1:** Modify the 370 Curriculum to allow students to specialize in a particular area of interest. The curriculum would be divided into three subspecialty areas called "Emphasis Tracks" as follows:

- Computer Security Emphasis Track
- Telecommunications Networks Emphasis Track
- Information Resource Management Emphasis Track

Each "Emphasis Track" would have one or more mandatory required courses and a variety of elective courses to choose from. The 370 Curriculum currently provides only one elective choice for students. The flexibility of being able to select from a variety of elective courses would allow the individual to tailor the curriculum to their particular field of interest. To promote this flexibility, two additional elective slots can be realized with the elimination of MN 4125 (Managing Planned Change in Complex Organizations) and IS 3171 (Economic Evaluation of Information Systems II). Examples of each Emphasis Track are provided below:

### **a. Computer Security Emphasis Track**

Required Courses:

IS 3220 - Computer Center Management

IS 4xxx<sup>3</sup> - Risk Analysis and Disaster Recovery Planning

**Elective Courses:**

- CS 4602 - Advanced Computer Security
- IS 3000 - Distributed Computer System
- IS 3503 - Micro-Computer Networks
- IS 4184 - Information Resource Management in DoN/DoD
- IS 4186 - Knowledge-Based Systems and Artificial Intelligence
- MN 4125 - Managing Planned Change in Complex Organizations
- OS 3404 - Man-Machine Interaction

**b. Telecommunications Networks Emphasis Track**

**Required Course:**

- IS 3000 - Distributed Computer System

**Elective Courses:**

- IS 3220 - Computer Center Management
- IS 3503 - Micro-Computer Networks
- IS 4184 - Information Resource Management in DoN/DoD
- IS 4xxx - Risk Analysis and Disaster Recovery Planning
- MN 4125 - Managing Planned Change in Complex Organizations
- OS 3404 - Man-Machine Interaction

**c. Information Resource Management Emphasis Track**

**Required Courses:**

- IS 4184 - Information Resource Management in DoN/DoD

**Elective Courses:**

- IS 3000 - Distributed Computer System
- IS 3220 - Computer Center Management

---

3. IS 4xxx Risk Analysis and Disaster Recovery Planning is a course that would have to be developed.

- IS 3503 - Micro-Computer Networks
- IS 4xxx - Risk Analysis and Disaster Recovery Planning
- MN 4125 - Managing Planned Change in Complex Organizations
- MN 4105 - Management Policy
- OS 3404 - Man-Machine Interaction

**Recommendation 2:** Eliminate the IS 3171 (Economic Evaluation of Informations Systems II), MN 3154 (Financial Management in the Armed Forces), and MN 4125 (Managing Planned Changed in Complex Organizations) courses from the 370 Curriculum and replace them with emphasis track electives. Split the CS 3030 Computer Architecture and Operating Systems course into two courses. One course would consist of primarily computer architecture, CS 3010, and the other course would consist primarily of operating systems, CS 3030.

The benefit of splitting the current CS 3030 Computer Architecture and Operating Systems course into two separate course will allow the instructors more time to present the material in greater detail as well as inject more security related issues. The only benefit of not splitting CS 3030 is that it would make room for a fourth Track Elective. Two curriculum matrices are shown in Tables 4 and 5. Table 4 reflects CS 3030 being split and Table 5 reflects CS 3030 not being split.



**Table 4: MATRIX WITH IS 3171, MN 3154, AND MN 4125  
ELIMINATED AND CS 3030 SPLIT**

<b>1 st Quarter</b>	<b>IS 2000 (3-1)</b> Introduction to Computer Management	<b>CS 2970 (4-1)</b> Structured Programming with Ada	<b>OS 3101 (4-1)</b> Statistical Analysis for Management	<b>MN 2155 (4-0)</b> Accounting for Management
<b>2 nd Quarter</b>	<b>CS 3010 (4-0)</b> Computer Architecture	<b>MA 1248 (4-1)</b> Selected Topics in Applied Mathematics	<b>OS 3004 (5-0)</b> Operations Research for Computer System Managers	<b>MN 3105 (4-0)</b> Organization and Management
<b>3 rd Quarter</b>	<b>IS 4200 (4-0)</b> System Analysis and Design	<b>EO 2710 (4-2)</b> Comm Systems I: Analog Signals and Systems	<b>IS 4183 (4-1)</b> Applications of Database Management Systems	<b>IS 3170 (4-0)</b> Economic Evaluation of Information Systems I
<b>4 th Quarter</b>	<b>IS 3020 (3-2))</b> Software Design	<b>EO 2750 (4-2)</b> Comm Systems II: Digital Signals and Systems	<b>IS 4185 (4-1)</b> Decision Support Systems	<b>CS 3030 (4-0)</b> Operating Systems
<b>5 th Quarter</b>	<b>IS 4300 (4-0)</b> Software Engineering and Management	<b>EO 3750 (4-0)</b> Communications System Analysis	<b>IS 3502 (4-0)</b> Computer Networks: Wide Area / Local Area	<b>CM 3112 (4-0)</b> Navy Telecommunications Systems
<b>6 th Quarter</b>	<b>Track Elective</b>	<b>NS 3252 (4-0)</b> Joint and Maritime Strategic Planning	<b>IS 4502 (4-0)</b> Telecommunications Network	<b>IS 0810 (0-0)</b> Thesis Research for Information Technology Management Students
<b>7 th Quarter</b>	<b>Track Elective</b>	<b>CS 4601 (4-0)</b> Computer Security	<b>MN 3307 (4-0)</b> ADP Acquisition	<b>IS 0810 (0-0)</b> Thesis Research for Information Technology Management Students
<b>8 th Quarter</b>	<b>IS 4182 (4-0)</b> Information Systems Management	<b>Track Elective</b>	<b>IS 0810 (0-0)</b> Thesis Research for Information Technology Management Students	<b>IS 0810 (0-0)</b> Thesis Research for Information Technology Management Students

**Table 5: MATRIX WITH IS 3171, MN 3154 AND MN 4125 ELIMINATED AND WITHOUT CS 3030 SPLIT**

<b>1 st Quarter</b>	<b>IS 2000 (3-1)</b> Introduction to Computer Management	<b>CS 2970 (4-1)</b> Structured Programming with Ada	<b>OS 3101 (4-1)</b> Statistical Analysis for Management	<b>MN 2155 (4-0)</b> Accounting for Management
<b>2 nd Quarter</b>	<b>CS 3030 (4-0)</b> Computer Architecture and Operating Systems	<b>MA 1248 (4-1)</b> Selected Topics in Applied Mathematics	<b>OS 3004 (5-0)</b> Operations Research for Computer Systems Managers	<b>MN 3105 (4-0)</b> Organization and Management
<b>3 rd Quarter</b>	<b>IS 4200 (4-0)</b> System Analysis and Design	<b>EO 2710 (4-2)</b> Comm Systems I: Analog Signals and Systems	<b>IS 4183 (4-1)</b> Applications of Database Management Systems	<b>IS 3170 (4-0)</b> Economic Evaluation of Information Systems I
<b>4 th Quarter</b>	<b>IS 3020 (3-2))</b> Software Design	<b>EO 2750 (4-2)</b> Comm Systems II: Digital Signals and Systems	<b>IS 4185 (4-1)</b> Decision Support Systems	<b>MN 3307 (4-0)</b> ADP Acquisition
<b>5 th Quarter</b>	<b>IS 4300 (4-0)</b> Software Engineering and Management	<b>EO 3750 (4-0)</b> Communications System Analysis	<b>IS 3502 (4-0)</b> Computer Networks: Wide Area / Local Area	<b>CM 3112 (4-0)</b> Navy Telecommunications Systems
<b>6 th Quarter</b>	<b>Track Elective</b>	<b>NS 3252 (4-0)</b> Joint and Maritime Strategic Planning	<b>IS 4502 (4-0)</b> Telecommunications Network	<b>IS 0810 (0-0)</b> Thesis Research for Information Technology Management Students
<b>7 th Quarter</b>	<b>Track Elective</b>	<b>CS 4601 (4-0)</b> Computer Security	<b>Track Elective</b>	<b>IS 0810 (0-0)</b> Thesis Research for Information Technology Management Students
<b>8 th Quarter</b>	<b>IS 4182 (4-0)</b> Information Systems Management	<b>Track Elective</b>	<b>IS 0810 (0-0)</b> Thesis Research for Information Technology Management Students	<b>IS 0810 (0-0)</b> Thesis Research for Information Technology Management Students

**Recommendation 3:** Establish an advanced computer security course as an elective for those individuals desiring to gain expertise in computer security. Academic objectives would include an understanding of:

- the fundamental models involved in multilevel security.
- how the fundamental models used in multilevel security are implemented in the design of a secure computer system.
- the advancements and limitations of computer security

technology in the areas of multilevel databases, networks and distributed systems.

- the various roles encryption plays in the development of secure network protocols and remote access control.
- the DoD requirements for trusted systems and the verification process.

**Recommendation 4:** Establish a Disaster Recovery and Planning course IS 4xxx, which would include:

- current theoretical foundations for conducting risk analysis.
- an introduction to automated assessment tools.
- an introduction to current guidelines and directives.
- analyses of case studies.

**Recommendation 5:** Establish a computer security laboratory, which would allow students to apply theoretical concepts. This lab would include:

- quarantined systems which would allow students to experiment with viruses without infecting other computers. Students could monitor the life cycle of viruses along with evaluating different anti-virus software packages.
- computers with communication software that would allow students to gain experience using both private and public key encryption protocols and permit them to conduct fundamental penetration testing.
- TEMPEST equipment to monitor electronic emanations from computer systems, peripherals, and conductors.
- a Honeywell Information System Secure Communications Processor (SCOMP). The SCOMP is the only system to date that has received an A1 Orange Book security rating. The SCOMP would provide students a vital research tool to explore multilevel

security issues.

- various biometric devices that measure human body characteristics used in computer security such as: retinal patterns, fingerprints, handprints, voice patterns, keystroke patterns, and signature dynamics. The Naval Postgraduate School's Operations Research Department has an excellent biometrics laboratory which could be used as an annex of the computer security laboratory.

**Recommendation 5:** Provide adequate funding in order to support a quarterly seminar program in which visiting specialists from both government and civilian sectors could address students and faculty concerning new technologies, products and policies.

**Recommendation 6:** Restructure the IS 2000 Introduction to Computer Management course to include high level coverage of material delineated in the (ISC)<sup>2</sup> certification format. This would expose new students to the importance of computer security early in the curriculum and thereby foster a basic understanding and appreciation of concepts that will be introduced in subsequent courses.

**Recommendation 7:** Use the Appendices A, B, and C as a computer security reference to help guide faculty members in modifying their courses to include relevant computer security topics.

## VII. CONCLUSION

DoD has become increasingly dependent upon storing its sensitive information in electronic form and naturally there is a deep concern for the integrity and privacy of this valuable information. In the recent aftermath of numerous electronic break-ins, the DoD continues to express anxiety over technically weak system administrators' inability to protect sensitive electronic information.

A significant step in minimizing electronic intrusions and bolstering computer security in DoD is to educate military officers and federal civilians in the latest technology and administrative controls available to enhance computer security. This can be accomplished by modifying the Information Technology Management (370) Curriculum at the Naval Postgraduate School to adhere to the proposed recommendations.

In order to further enhance the Information Technology Management (370) Curriculum at the Naval Postgraduate School, and strengthen the graduate's knowledge of computer security, it is imperative that the 370 Curriculum be revised to meet the needs of DoD in this rapidly changing technology.

# APPENDIX A

**Table 6: Information Systems Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	IS 2000	IS 3020	IS 3170	IS 3171	IS 3502	IS 4182	IS 4183	IS 4185	IS 4200	IS 4300	IS 4502
<b>I. Overview</b>											
<b>A. Development of a Security Program</b>											
<b>1. Reason for a organizational security management policy</b>											
<b>a. Objectives</b>											
1. Identify sensitive systems/data	+					+					
2. Security plan	+					+					
3. Training	+					+					
<b>b. Policies</b>											
1. Written and communicated						+					
2. Board of directors responsibility						+					
3. DPMA model policy						+					
<b>c. Connectivity, organizational structure, and security</b>											
1. Connectivity defined						+					
2. Effect on organizational structure						+					
3. Security considerations						+					
<b>d. Plans</b>											
1. Human resource management	+					+					
2. Access control	+					+					
3. Data control	+					+					

**Table 6: Information Systems Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	IS 2000	IS 3020	IS 3170	IS 3171	IS 3502	IS 4182	IS 4183	IS 4185	IS 4200	IS 4300	IS 4502
4. Labeling	+					+					
5. Contingency plan	+					+					
6. Legal responsibilities	+					+					
e. Responsibilities											
1. Board of Directors						+					
2. Board of Directors & senior management						+					
3. Middle management						+					
4. Users						+					
B. Risk Analysis											
1. Reason	+					+					
2. Typical contents	+					+					
3. Main purposes	+					+					
C. Contingency Planning											
1. Defined	+					+					
2. Backup	+					+					
3. Critical elements	+					+					
D. Legal Issues for Managers											
1. Licenses						+					
2. Fraud/misuse						+					

**Table 6: Information Systems Courses**

<b>COMPUTER SECURITY CONCEPTS AND ISSUES</b>	<b>IS 2000</b>	<b>IS 3020</b>	<b>IS 3170</b>	<b>IS 3171</b>	<b>IS 3502</b>	<b>IS 4182</b>	<b>IS 4183</b>	<b>IS 4185</b>	<b>IS 4200</b>	<b>IS 4300</b>	<b>IS 4502</b>
3. Privacy						+					
4. Copyright						+					
5. Trade secrets						+					
6. Employee agreements						+					
<b>E. System Validation &amp; Verification (Accreditation)</b>											
1. Plan testing						+					
2. Acceptance of responsibility						+					
<b>F. Information Systems Audit</b>						+					
<b>II. Risk Management</b>											
<b>A. Asset Identification and Valuation</b>											
1. Processing valuation			+			+					
2. Risk management team			+			+					
3. Classification of assets			+			+					
4. Subclassification of assets											
a. People, skills, and procedures			+			+					
b. Physical and environmental			+			+					
c. Communications			+			+					
d. Hardware			+			+					
e. Software			+			+					
f. Data and information			+			+					



**Table 6: Information Systems Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	IS 2000	IS 3020	IS 3170	IS 3171	IS 3502	IS 4182	IS 4183	IS 4185	IS 4200	IS 4300	IS 4502
g. Goodwill			+			+					
5. Determining values for assets											
a. Acquired and intrinsic values			+			+					
b. Purpose of assigning value to assets			+			+					
c. How to measure assets values			+			+					
d. Criticality and sensitivity											
1. Criticality: business impact, revenue losses			+			+					
embarrassment, legal problems											
2. Sensitivity: privacy, trade secrets, planning			+			+					
information, financial data											
3. Sources MIS, users, senior management			+			+					
4. Levels: military, national security, commercial			+			+					
e. Asset valuation: standard accounting			+			+					
f. Asset valuation: replacement value			+			+					
g. Asset valuation: loss of availability			+			+					
h. Asset valuation: estimating methods			+			+					
6. Use of asset analysis results											
a. Limitations											
1. Lack of data			+			+					

**Table 6: Information Systems Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	IS 2000	IS 3020	IS 3170	IS 3171	IS 3502	IS 4182	IS 4183	IS 4185	IS 4200	IS 4300	IS 4502
2. Interpretation			+			+					
<b>B. Threat and Exposure Assessment</b>											
1. Threats, vulnerabilities, and exposures defined						+					
2. Methodologies for threat assessment											
a. Properties of threats						+					
b. Properties of assets						+					
c. Combining properties: the cost exposure matrix						+					
3. Probability concepts											
a. Definitions						+					
b. Tables of probability values						+					
c. Fuzzy metrics						+					
d. Expected values						+					
e. Worst case						+					
f. Automated packages						+					
4. Sources of threat information											
a. Vulnerability analysis						+					
b. Scenarios						+					
c. Past history						+					
d. Outside Sources						+					
5. Calculating exposures						+					

**Table 6: Information Systems Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	IS 2000	IS 3020	IS 3170	IS 3171	IS 3502	IS 4182	IS 4183	IS 4185	IS 4200	IS 4300	IS 4502
<b>III. Safeguards: Security and Control Measures</b>											
<b>A. Overview of Safeguards</b>											
1. Common sense	+					+					
2. Types of controls: prevention, detection, reaction											
a. Basic purpose of controls	+					+					
b. Prevention	+					+					
c. Detection	+					+					
d. Containment	+					+					
e. Reaction or correction	+					+					
3. Design strategies											
a. Countermeasures	+					+					
b. Countermeasure selection						+					
c. Sensitivity analysis						+					
d. Decision analysis						+					
e. Goal-seeking heuristics						+					
f. Risk perception and communication						+					
4. Components of EDP security											
a. Administrative and organizational controls						+					
b. Policies						+					

**Table 6: Information Systems Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	IS 2000	IS 3020	IS 3170	IS 3171	IS 3502	IS 4182	IS 4183	IS 4185	IS 4200	IS 4300	IS 4502
c. Personnel						+					
d. Physical and environmental security						+					
e. Computer operations						+					
f. Contingency planning						+					
5. Components of EDP security: technical											
a. Communication and electronic exposures						+					
b. Hardware						+					
c. Encryption						+					
d. Software						+					
B. Organizational and Administrative Controls											
1. Trade secrets, employee agreements, conflict of interest						+					
2. Security policy											
a. Intent (related to sensitivity)						+					
b. Access to and distribution of information						+					
c. Laws						+					
d. Regulations						+					
e. Company policy						+					
f. Mandatory and discretionary security						+					
g. Accountability: identification, authentication, audit						+					
3. Responsibility areas, System Security Officer											

**Table 6: Information Systems Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES		IS 2000	IS 3020	IS 3170	IS 3171	IS 3502	IS 4182	IS 4183	IS 4185	IS 4200	IS 4300	IS 4502
a.	Basic role	+					+					
b.	Duties	+					+					
c.	Training and skills for a System Security Office	+					+					
4.	Employee training											
a.	Orientation						+					
b.	Skills						+					
5.	Telecommuting						+					
C.	Personnel Consideration											
1.	Human motives for criminal action	+					+					
2.	Employee selection											
a.	Application forms						+					
b.	Permissions for investigations						+					
c.	Security clearance and citizenship						+					
3.	Professional certificates						+					
4.	Working environment											
a.	Vacations and job rotation						+					
b.	Employee-management relations						+					
c.	Career path planning						+					
d.	Remuneration						+					

**Table 6: Information Systems Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	IS 2000	IS 3020	IS 3170	IS 3171	IS 3502	IS 4182	IS 4183	IS 4185	IS 4200	IS 4300	IS 4502
5. Access rights and privileges	+					+					
6. Prosecution for adverse actions	+					+					
7. Employee separation						+					
D. Physical and Environmental Security											
1. Site location and construction											
a. Computer room considerations	+	+				+					
b. Special microcomputer problems			+			+					
2. Physical access											
a. Access vs. security	+	+				+					
b. Rooms, windows, doors, keys			+			+					
3. Power											
a. Spikes, surges, brownouts	+	+				+					
b. Costs of prevention/protection equipment			+			+					
4. Air-conditioning	+	+				+					
5. Water exposures and problems	+	+				+					
6. Fire prevention	+	+				+					
7. Fire protection			+			+					
8. Tape and media libraries; retention policies			+			+					
9. Waste disposal			+			+					
10. Off-site storage			+			+					

**Table 6: Information Systems Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	IS 2000	IS 3020	IS 3170	IS 3171	IS 3502	IS 4182	IS 4183	IS 4185	IS 4200	IS 4300	IS 4502
11. Document libraries and controls			+			+					
<b>E. Computer Operations</b>						+					
1. Organization of computer operations											
a. Mainframes						+					
b. Minicomputers						+					
c. Microcomputers/office automation						+					
2. Separation of duties						+					
3. Controls at interfaces						+					
4. Media controls						+					
5. Backup procedures						+					
6. People controls						+					
<b>F. Contingency Planning</b>											
1. Backups and procedures											
a. Data		+				+					
b. Manuals and documentation		+				+					
c. Equipment		+				+					
1. Air conditioning		+				+					
2. Uninterruptible power supply		+				+					
2. Catastrophe planning											

**Table 6: Information Systems Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	IS 2000	IS 3020	IS 3170	IS 3171	IS 3502	IS 4182	IS 4183	IS 4185	IS 4200	IS 4300	IS 4502
a. Stages in a disaster		+				+					
b. Planning and response teams		+				+					
c. Testing plan		+				+					
d. Communication of plan		+				+					
3. Security and controls in off-site backup and facilities		+				+					
4. Business and DP insurance		+				+					
5. Software escrow arrangements											
<b>IV. Safeguards: Security and Control Measures, Technical</b>											
A. Hackers and reality: Perception of Risk		+									
B. Communications and Electronic Exposures											
1. Locus of attack											
a. Terminals							+				+
b. Hosts							+				+
c. Front-end processors							+				+
d. Gateways							+				+
e. Links							+				+
f. Switches (multiplexors, packet switching, etc.)							+				+
g. Special problems with intelligent workstations							+				+
2. Types of attack											
a. Passive: disclosure; traffic analysis; add/remove nodes							+				+



**Table 6: Information Systems Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	IS 2000	IS 3020	IS 3170	IS 3171	IS 3502	IS 4182	IS 4183	IS 4185	IS 4200	IS 4300	IS 4502
b. Active: modification; insertion; deletion; replay							+				+
3. Electronic											
a. Incoming: interruptions; static; FRI; EMP							+				+
b. Outgoing: leakage							+				+
c. Solutions: shielding							+				+
4. Communications											
a. Value-added communications							+				+
b. exposures incoming: noise and interference							+				+
c. Exposures outgoing: interception, replacement							+				+
d. Solution: physical measures							+				+
e. Solutions: encryption							+				+
f. ISO OSI communications standards							+				+
5. Network design											
a. Design considerations											
1. Integration of countermeasures into network	+						+				+
design: cryptographic checksum; time stamp;											
Bell/LaPadula model											
2. Integration of countermeasures into protocol layers:							+				+
link level encryption: end-to-end encryption											

**Table 6: Information Systems Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	IS 2000	IS 3020	IS 3170	IS 3171	IS 3502	IS 4182	IS 4183	IS 4185	IS 4200	IS 4300	IS 4502
<b>b. Assurance</b>											
1. Concept of trust	+						+				+
2. Degrees of trustworthiness	+						+				+
3. Trusted network base	+						+				+
4. Testing							+				+
5. Formal specification							+				+
6. Formal verification							+				+
<b>C. Encryption</b>											
1. Definition (plaintext, ciphertext; encryption/decryption)	+						+				+
2. Public key and private key	+						+				+
3. Key distribution							+				+
4. Link level, end-to-end							+				+
5. Block mode, cipher block chaining, stream ciphers (synchronous and self-synchronous)							+				+
6. DES, RSA	+						+				+
7. Cryptanalysis and strength of ciphers (theoretically secure, computationally secure)							+				+
8. Advantages and disadvantages							+				+
<b>D. Software and Operating System Controls</b>											
1. Secure operating systems											

**Table 6: Information Systems Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	IS 2000	IS 3020	IS 3170	IS 3171	IS 3502	IS 4182	IS 4183	IS 4185	IS 4200	IS 4300	IS 4502
a. History	+	+									+
b. Concepts: capabilities, reference validations											
1. Secure kernels		+									
2. Reference validations and capabilities		+									
c. Present guidelines and standards, trusted computer base		+									+
d. Design principles fro secure systems											
1. Least privilege											
2. Open design											
3. Fail-safe defaults											
4. Economy of mechanisms											
5. Naturalness (human factors)											
6. Continuous protection											
e. Common penetration methods and countermeasures											
1. Trojan horse; virus; worm; salami; piggyback;	+	+									
deception; human compromise; etc.											
2. Controls on changes; audit trails; program library;		+									
code comparison; checksums and encryption;											
vaccines and antiviral agents; access control; etc.											
2. Access control											

**Table 6: Information Systems Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	IS 2000	IS 3020	IS 3170	IS 3171	IS 3502	IS 4182	IS 4183	IS 4185	IS 4200	IS 4300	IS 4502
a. Discretionary access control											
1. Subjects and objects									■		
2. Access privileges									■		
3. Granting/revoking of privileges									■		
4. Access control lists									■		
5. Capabilities, descriptors									■		
6. Supervisor states, rings, domains									■		
b. Non-discretionary access control											
1. Labels on subjects, objects									■		
2. Rules for reading, writing									■		
3. Software Controls: Development											
a. The real problem: bugs		+	+						■		+
b. Software engineering principles: layering, modularity		+							■		+
c. Structured methods		+							■		+
d. Formal specification and verification		+							■		+
e. Program library/librarian		+							■		+
f. Data dictionary as a control		+							■		+
g. Conversion and implementation		+							■		+
4. Software controls: Maintenance											
a. Separation of duties		+							■		+

**Table 6: Information Systems Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	IS 2000	IS 3020	IS 3170	IS 3171	IS 3502	IS 4182	IS 4183	IS 4185	IS 4200	IS 4300	IS 4502
b. Testing controls		+							+		
c. Change control		+							+		
5. Assurance											
a. Integrity		+							+		
b. Testing		+							+		
c. Specification/verification		+							+		
d. Facility management		+							+		
e. Disaster/contingency		+							+		
f. Compliance/degree of trust		+							+		
E. Database systems security											
1. Overview											
a. Review of basic concepts of information protection		+	+					+			+
b. Role of information protection in database systems		+	+					+			+
2. Threats											
a. Direct disclosure of data								+			
b. Modification of data/tampering with data								+			
c. Inference								+			
d. Aggregation								+			
e. Trojan horse								+			

**Table 6: Information Systems Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	IS 2000	IS 3020	IS 3170	IS 3171	IS 3502	IS 4182	IS 4183	IS 4185	IS 4200	IS 4300	IS 4502
f. Covert disclosure of data							+				
3. Policy/mechanism											
a. Policy versus mechanism							+				
b. Access controls											
1. Access right and privileges							+				
2. Access control policies							+				
3. Granularity							+				
4. Labels							+				
5. Access control mechanisms							+				
c. Inference controls											
d. Integrity controls											
1. Integrity policy							+				
2. Integrity mechanisms							+				
e. Accountability controls											
1. Identification and authentication							+				
2. Audit							+				
4. Design issues											
a. Protection Approaches											
1. Trusted kernel		+					+				
2. Trusted filter		+					+				

**Table 6: Information Systems Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	IS 2000	IS 3020	IS 3170	IS 3171	IS 3502	IS 4182	IS 4183	IS 4185	IS 4200	IS 4300	IS 4502
3. Encryption		+					+				
b. Performance		+					+				
c. Storage		+					+				
d. Access control vs. integrity		+					+				
e. Assurance		+					+				
<b>V. Legal Environment and Professionalism</b>											
A. Law and legislation											
1. The underlying problem											
a. Theft, copying software, privacy		+					+				
b. Fraud							+				
c. Physical abuse							+				
d. Misuse of information							+				
e. Sabotage							+				
2. Laws as tools for computer security											
a. Privacy laws and legislation							+				
b. Intellectual property laws											
1. Copyright law							+				
2. Trade secret law							+				
3. Patent law							+				

**Table 6: Information Systems Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	IS 2000	IS 3020	IS 3170	IS 3171	IS 3502	IS 4182	IS 4183	IS 4185	IS 4200	IS 4300	IS 4502
4. Trademark law						+					
c. Federal laws (esp. Computer Security Act 1987)	+					+					
d. State statutes						+					
e. DPMA Model Computer Crime Bill						+					
f. Computer crime legislation in other countries						+					
3. Legislation as legal options to control computer crime											
a. License agreements (consumer license agreements)						+					
b. permanent license agreements						+					
c. Intellectual property rights						+					
d. Employee non-disclosure considerations						+					
e. Contracts											
1. Software development contracts						+					
2. Legal aspects of software purchasing						+					
3. Leasing contracts						+					
f. Warranties for software and hardware						+					
4. Control of strategic materials						+					
5. Fraud and crime prevention and detection						+					
6. Investigation; evidentiary trial						+					
B. Ethics and professionalism											
1. Ethical decision-making						+					



**Table 6: Information Systems Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	IS 2000	IS 3020	IS 3170	IS 3171	IS 3502	IS 4182	IS 4183	IS 4185	IS 4200	IS 4300	IS 4502
2. Professional societies											
a. British Computer Society						+					
b. North America: DPMA and ICCP						+					
c. Canada: CIPS and DPMA											
1. CIPS						+					
2. DPMA Canada						+					
d. Computer Professionals for Social Responsibility						+					
e. EDP Auditors Foundation						+					
3. National Computer Security Center						+					
4. National Bureau of Standards						+					
5. Certificate in Data Processing(CPC); Certified Information Systems Auditor (CISA)						+					
<b>VI. CICA Computer Control Guidelines</b>											
A. Accounting and auditing											
1. Computer Control Guidelines											
a. Responsibility for Control						+					
b. Information Systems Development and Acquisition						+					
c. Information Systems Processing						+					
d. Segregation of Incompatible Functions and Controls						+					

**Table 6: Information Systems Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	IS 2000	IS 3020	IS 3170	IS 3171	IS 3502	IS 4182	IS 4183	IS 4185	IS 4200	IS 4300	IS 4502
e. Application Controls						+					
2. Information systems audit											
a. Security review objectives						+					
b. Specific security controls						+					
c. Security review process						+					
d. Evidence accumulation						+					
e. Evaluation of test results						+					
f. Communication of control weaknesses						+					

# APPENDIX B

**Table 7: Computer Science Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	CS 2970	CS 3030	CS 4601
<b>I. Overview</b>			
<b>A. Development of a Security Program</b>			
1. Reason for a organizational security management policy			
a. Objectives			
1. Identify sensitive systems/data			
2. Security plan			
3. Training			
b. Policies			
1. Written and communicated			
2. Board of directors responsibility			
3. DPMA model policy			
c. Connectivity, organizational structure, and security			
1. Connectivity defined			
2. Effect on organizational structure			
3. Security considerations			
d. Plans			
1. Human resource management			
2. Access control			
3. Data control			

**Table 7: Computer Science Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES		CS 2970	CS 3030	CS 4601
4.	Labeling			
5.	Contingency plan			
6.	Legal responsibilities			
e.	Responsibilities			
1.	Board of Directors			
2.	Board of Directors & senior management			
3.	Middle management			
4.	Users			
B.	Risk Analysis			
1.	Reason			
2.	Typical contents			
3.	Main purposes			
C.	Contingency Planning			
1.	Defined			
2.	Backup			
3.	Critical elements			
D.	Legal Issues for Managers			
1.	Licenses			
2.	Fraud/misuse			

**Table 7: Computer Science Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	CS 2970	CS 3030	CS 4601
3. Privacy			
4. Copyright			
5. Trade secrets			
6. Employee agreements			
<b>E. System Validation &amp; Verification (Accreditation)</b>			
1. Plan testing			
2. Acceptance of responsibility			
<b>F. Information Systems Audit</b>			
<b>II. Risk Management</b>			
<b>A. Asset Identification and Valuation</b>			
1. Processing valuation			
2. Risk management team			
3. Classification of assets			
4. Subclassification of assets			
a. People, skills, and procedures			
b. Physical and environmental			
c. Communications			
d. Hardware			
e. Software			
f. Data and information			

**Table 7: Computer Science Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES		CS 2970	CS 3030	CS 4601
g.	Goodwill			<input checked="" type="checkbox"/>
5.	Determining values for assets			
a.	Acquired and intrinsic values			<input checked="" type="checkbox"/>
b.	Purpose of assigning value to assets			<input checked="" type="checkbox"/>
c.	How to measure assets values			<input checked="" type="checkbox"/>
d.	Criticality and sensitivity			
1.	Criticality: business impact, revenue losses			<input checked="" type="checkbox"/>
	embarrassment, legal problems			
2.	Sensitivity: privacy, trade secrets, planning			<input checked="" type="checkbox"/>
	information, financial data			
3.	Sources MIS, users, senior management			
4.	Levels: military, national security, commercial			<input checked="" type="checkbox"/>
e.	Asset valuation: standard accounting			<input checked="" type="checkbox"/>
f.	Asset valuation: replacement value			<input checked="" type="checkbox"/>
g.	Asset valuation: loss of availability			<input checked="" type="checkbox"/>
h.	Asset valuation: estimating methods			<input checked="" type="checkbox"/>
6.	Use of asset analysis results			
a.	Limitations			
1.	Lack of data			<input checked="" type="checkbox"/>

**Table 7: Computer Science Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	CS 2970	CS 3030	CS 4601
2. Interpretation			
B. Threat and Exposure Assessment			
1. Threats, vulnerabilities, and exposures defined			
2. Methodologies for threat assessment			
a. Properties of threats			
b. Properties of assets			
c. Combining properties: the cost exposure matrix			
3. Probability concepts			
a. Definitions			
b. Tables of probability values			
c. Fuzzy metrics			
d. Expected values			
e. Worst case			
f. Automated packages			
4. Sources of threat information			
a. Vulnerability analysis			
b. Scenarios			
c. Past history			
d. Outside Sources			
5. Calculating exposures			

**Table 7: Computer Science Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	CS 2970	CS 3030	CS 4601
<b>III. Safeguards: Security and Control Measures</b>			
<b>A. Overview of Safeguards</b>			
1. Common sense	✓		✓
2. Types of controls: prevention, detection, reaction			
a. Basic purpose of controls	✓		
b. Prevention	✓		
c. Detection	✓		
d. Containment			
e. Reaction or correction			
3. Design strategies			
a. Countermeasures			✓
b. Countermeasure selection			✓
c. Sensitivity analysis			
d. Decision analysis			
e. Goal-seeking heuristics			
f. Risk perception and communication			✓
4. Components of EDP security			
a. Administrative and organizational controls			✓
b. Policies			



**Table 7: Computer Science Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	CS 2970	CS 3030	CS 4601
c. Personnel			
d. Physical and environmental security			
e. Computer operations			
f. Contingency planning			
5. Components of EDP security: technical			
a. Communication and electronic exposures			
b. Hardware			
c. Encryption			
d. Software			
B. Organizational and Administrative Controls			
1. Trade secrets, employee agreements, conflict of interest			
2. Security policy			
a. Intent (related to sensitivity)			
b. Access to and distribution of information			
c. Laws			
d. Regulations			
e. Company policy			
f. Mandatory and discretionary security			
g. Accountability: identification, authentication, audit			
3. Responsibility areas, System Security Officer			

**Table 7: Computer Science Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES		CS 2970	CS 3030	CS 4601
a.	Basic role			
b.	Duties			
c.	Training and skills for a System Security Office			
4.	Employee training			
a.	Orientation			
b.	Skills			
5.	Telecommuting			
C.	Personnel Consideration			
1.	Human motives for criminal action			
2.	Employee selection			
a.	Application forms			
b.	Permissions for investigations			
c.	Security clearance and citizenship			
3.	Professional certificates			
4.	Working environment			
a.	Vacations and job rotation			
b.	Employee-management relations			
c.	Career path planning			
d.	Remuneration			

**Table 7: Computer Science Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	CS 2970	CS 3030	CS 4601
5. Access rights and privileges			
6. Prosecution for adverse actions			
7. Employee separation			
D. Physical and Environmental Security			
1. Site location and construction			
a. Computer room considerations			
b. Special microcomputer problems			
2. Physical access			
a. Access vs. security			
b. Rooms, windows, doors, keys			
3. Power			
a. Spikes, surges, brownouts			
b. Costs of prevention/protection equipment			
4. Air-conditioning			
5. Water exposures and problems			
6. Fire prevention			
7. Fire protection			
8. Tape and media libraries; retention policies			
9. Waste disposal			
10. Off-site storage			

**Table 7: Computer Science Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES		CS 2970	CS 3030	CS 4601
11. Document libraries and controls				✓
<b>E. Computer Operations</b>				
1. Organization of computer operations				
a. Mainframes				
b. Minicomputers				
c. Microcomputers/office automation				
2. Separation of duties				
3. Controls at interfaces				
4. Media controls				
5. Backup procedures				✓
6. People controls				
<b>F. Contingency Planning</b>				
1. Backups and procedures				
a. Data				✓
b. Manuals and documentation				✓
c. Equipment				
1. Air conditioning				
2. Uninterruptible power supply				
2. Catastrophe planning				

**Table 7: Computer Science Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	CS 2970	CS 3030	CS 4601
a. Stages in a disaster			✓
b. Planning and response teams			✓
c. Testing plan			✓
d. Communication of plan			✓
3. Security and controls in off-site backup and facilities			✓
4. Business and DP insurance			✓
5. Software escrow arrangements			
<b>IV. Safeguards: Security and Control Measures, Technical</b>			
A. Hackers and reality: Perception of Risk			✓
B. Communications and Electronic Exposures			
1. Locus of attack			
a. Terminals			
b. Hosts			
c. Front-end processors			
d. Gateways			
e. Links			
f. Switches (multiplexors, packet switching, etc.)			
g. Special problems with intelligent workstations			
2. Types of attack			
a. Passive: disclosure; traffic analysis; add/remove nodes			✓

**Table 7: Computer Science Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES		CS 2970	CS 3030	CS 4601
	b. Active: modification; insertion; deletion; replay			✓
3.	Electronic			
	a. Incoming: interruptions; static; FRI; EMP			✓
	b. Outgoing: leakage			✓
	c. Solutions: shielding			✓
4.	Communications			
	a. Value-added communications			
	b. exposures incoming: noise and interference			
	c. Exposures outgoing: interception, replacement			
	d. Solution: physical measures			
	e. Solutions: encryption			
	f. ISO OSI communications standards			
5.	Network design			
	a. Design considerations			
	1. Integration of countermeasures into network			
	design: cryptographic checksum; time stamp;			
	Bell/LaPadula model			
	2. Integration of countermeasures into protocol layers:			
	link level encryption; end-to-end encryption			

**Table 7: Computer Science Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES		CS 2970	CS 3030	CS 4601
b. Assurance				
1. Concept of trust				
2. Degrees of trustworthiness				
3. Trusted network base				
4. Testing				
5. Formal specification				✓
6. Formal verification				✓
C. Encryption				
1. Definition (plaintext, ciphertext; encryption/decryption)				✓
2. Public key and private key				✓
3. Key distribution				✓
4. Link level, end-to-end				✓
5. Block mode, cipher block chaining, stream ciphers (synchronous and self-synchronous)				✓
6. DES, RSA				✓
7. Cryptanalysis and strength of ciphers (theoretically secure computationally secure)				✓
8. Advantages and disadvantages				✓
D. Software and Operating System Controls				
1. Secure operating systems				

**Table 7: Computer Science Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES		CS 2970	CS 3030	CS 4601
a.	History			S
b.	Concepts: capabilities, reference validations			
1.	Secure kernels			✓
2.	Reference validations and capabilities		+	✓
c.	Present guidelines and standards, trusted computer base		+	✓
d.	Design principles fro secure systems			
1.	Least privilege		+	✓
2.	Open design		+	✓
3.	Fail-safe defaults		+	
4.	Economy of mechanisms		+	
5.	Naturalness (human factors)		+	
6.	Continuous protection		+	
e.	Common penetration methods and countermeasures			
1.	Trojan horse; virus; worm; salami; piggyback; deception; human compromise; etc.		+	+
2.	Controls on changes: audit trails; program library; code comparison; checksums and encryption; vaccines and antiviral agents; access control; etc.		+	✓
2.	Access control			



**Table 7: Computer Science Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	CS 2970	CS 3030	CS 4601
a. Discretionary access control			
1. Subjects and objects		+	█
2. Access privileges		+	█
3. Granting/revoking of privileges		+	█
4. Access control lists		+	█
5. Capabilities, descriptors		+	█
6. Supervisor states, rings, domains		+	█
b. Non-discretionary access control			
1. Labels on subjects, objects		+	█
2. Rules for reading, writing		+	█
3. Software Controls: Development			
a. The real problem: bugs		+	█
b. Software engineering principles: layering, modularity		+	█
c. Structured methods		+	█
d. Formal specification and verification		+	█
e. Program library/librarian		+	
f. Data dictionary as a control		+	
g. Conversion and implementation		+	
4. Software controls: Maintenance			
a. Separation of duties		+	

**Table 7: Computer Science Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES		CS 2970	CS 3030	CS 4601
b.	Testing controls	+		
c.	Change control	+		
5.	Assurance			
a.	Integrity	+		✓
b.	Testing	+		✓
c.	Specification/verification	+		✓
d.	Facility management			
e.	Disaster/contingency			
f.	Compliance/degree of trust			
E.	Database systems security			
1.	Overview			
a.	Review of basic concepts of information protection			✓
b.	Role of information protection in database systems			✓
2.	Threats			
a.	Direct disclosure of data			✓
b.	Modification of data/tampering with data			✓
c.	Inference			✓
d.	Aggregation			✓
e.	Trojan horse			✓

**Table 7: Computer Science Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	CS 2970	CS 3030	CS 4601
f. Covert disclosure of data			✓
3. Policy/mechanism			
a. Policy versus mechanism			
b. Access controls			
1. Access right and privileges			✓
2. Access control policies			
3. Granularity			
4. Labels			
5. Access control mechanisms			✓
c. Inference controls			✓
d. Integrity controls			
1. Integrity policy			✓
2. Integrity mechanisms			
e. Accountability controls			
1. Identification and authentication			
2. Audit			
4. Design issues			
a. Protection Approaches			
1. Trusted kernel			✓
2. Trusted filter			

**Table 7: Computer Science Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	CS 2970	CS 3030	CS 4601
3. Encryption			
b. Performance			
c. Storage			
d. Access control vs. integrity			
e. Assurance			
<b>V. Legal Environment and Professionalism</b>			
A. Law and legislation			
1. The underlying problem			
a. Theft, copying software, privacy			
b. Fraud			
c. Physical abuse			
d. Misuse of information			
e. Sabotage			
2. Laws as tools for computer security			
a. Privacy laws and legislation			
b. Intellectual property laws			
1. Copyright law			
2. Trade secret law			
3. Patent law			

**Table 7: Computer Science Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES		CS 2970	CS 3030	CS 4601
4. Trademark law				✓
c. Federal laws (esp. Computer Security Act 1987)				✓
d. State statutes				
e. DPMA Model Computer Crime Bill				
f. Computer crime legislation in other countries				
3. Legislation as legal options to control computer crime				
a. License agreements (consumer license agreements)				✓
b. permanent license agreements				✓
c. Intellectual property rights				✓
d. Employee non-disclosure considerations				
e. Contracts				
1. Software development contracts				
2. Legal aspects of software purchasing				
3. Leasing contracts				
f. Warranties for software and hardware				
4. Control of strategic materials				
5. Fraud: crime prevention and detection				
6. Investigation: evidentiary trial				
B. Ethics and professionalism				
1. Ethical decision-making		+		

**Table 7: Computer Science Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	CS 2970	CS 3030	CS 4601
2. Professional societies			
a. British Computer Society			
b. North America: DPMA and ICCP			
c. Canada: CIPS and DPMA			
1. CIPS			
2. DPMA Canada			
d. Computer Professionals for Social Responsibility			
e. EDP Auditors Foundation			
3. National Computer Security Center			
4. National Bureau of Standards			
5. Certificate in Data Processing(CPC); Certified Information Systems Auditor(CISA)			
<b>VI. CICA Computer Control Guidelines</b>			
A. Accounting and auditing			
1. Computer Control Guidelines			
a. Responsibility for Control			
b. Information Systems Development and Acquisition			
c. Information Systems Processing			
d. Segregation of Incompatible Functions and Controls			

**Table 7: Computer Science Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES		CS 2970	CS 3030	CS 4601
e.	Application Controls			
2.	Information systems audit			
a.	Security review objectives			
b.	Specific security controls			
c.	Security review process			
d.	Evidence accumulation			
e.	Evaluation of test results			
f.	Communication of control weaknesses			

# APPENDIX C

**Table 8: Electro-Optical and Communication Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	EO 2710	EO 2750	EO 3750	CM 3112
<b>I. Overview</b>				
<b>A. Development of a Security Program</b>				
<b>1. Reason for a organizational security management policy</b>				
<b>a. Objectives</b>				
<b>1. Identify sensitive systems/data</b>				
<b>2. Security plan</b>				
<b>3. Training</b>				
<b>b. Policies</b>				
<b>1. Written and communicated</b>				
<b>2. Board of directors responsibility</b>				
<b>3. DPMA model policy</b>				
<b>c. Connectivity, organizational structure, and security</b>				
<b>1. Connectivity defined</b>				
<b>2. Effect on organizational structure</b>				
<b>3. Security considerations</b>				
<b>d. Plans</b>				
<b>1. Human resource management</b>				
<b>2. Access control</b>				
<b>3. Data control</b>				



**Table 8: Electro-Optical and Communication Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	EO 2710	EO 2750	EO 3750	CM 3112
4. Labeling				
5. Contingency plan				
6. Legal responsibilities				
e. Responsibilities				
1. Board of Directors				
2. Board of Directors & senior management				
3. Middle management				
4. Users				
B. Risk Analysis				
1. Reason				
2. Typical contents				
3. Main purposes				
C. Contingency Planning				
1. Defined				
2. Backup				
3. Critical elements				
D. Legal Issues for Managers				
1. Licenses				
2. Fraud/misuse				

**Table 8: Electro-Optical and Communication Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	EO 2710	EO 2750	EO 3750	CM 3112
3. Privacy				
4. Copyright				
5. Trade secrets				
6. Employee agreements				
E. System Validation & Verification (Accreditation)				
1. Plan testing				
2. Acceptance of responsibility				
F. Information Systems Audit				
<b>II. Risk Management</b>				
A. Asset Identification and Valuation				
1. Processing valuation				
2. Risk management team				
3. Classification of assets				
4. Subclassification of assets				
a. People, skills, and procedures				
b. Physical and environmental				
c. Communications				
d. Hardware				
e. Software				
f. Data and information				

**Table 8: Electro-Optical and Communication Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	EO 2710	EO 2750	EO 3750	CM 3112
g. Goodwill				
5. Determining values for assets				
a. Acquired and intrinsic values				
b. Purpose of assigning value to assets				
c. How to measure assets values				
d. Criticality and sensitivity				
1. Criticality: business impact, revenue losses				
embarrassment, legal problems				
2. Sensitivity: privacy, trade secrets, planning				
information, financial data				
3. Sources MIS, users, senior management				
4. Levels: military, national security, commercial				
e. Asset valuation: standard accounting				
f. Asset valuation: replacement value				
g. Asset valuation: loss of availability				
h. Asset valuation: estimating methods				
6. Use of asset analysis results				
a. Limitations				
1. Lack of data				

**Table 8: Electro-Optical and Communication Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	EO 2710	EO 2750	EO 3750	CM 3112
2. Interpretation				
B. Threat and Exposure Assessment				
1. Threats, vulnerabilities, and exposures defined				
2. Methodologies for threat assessment				
a. Properties of threats				
b. Properties of assets				
c. Combining properties: the cost exposure matrix				
3. Probability concepts				
a. Definitions				
b. Tables of probability values				
c. Fuzzy metrics				
d. Expected values				
e. Worst case				
f. Automated packages				
4. Sources of threat information				
a. Vulnerability analysis				
b. Scenarios				
c. Past history				
d. Outside Sources				
5. Calculating exposures				

**Table 8: Electro-Optical and Communication Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	EO 2710	EO 2750	EO 3750	CM 3112
<b>III. Safeguards: Security and Control Measures</b>				
<b>A. Overview of Safeguards</b>				
1. Common sense	+			
2. Types of controls: prevention, detection, reaction				
a. Basic purpose of controls	+			
b. Prevention	+			
c. Detection	+			
d. Continuum	+			
e. Reaction or correction	+			
3. Design strategies				
a. Countermeasures	+			
b. Countermeasure selection	+			
c. Sensitivity analysis				
d. Decision analysis				
e. Goal-seeking heuristics				
f. Risk perception and communication				
4. Components of EDP security				
a. Administrative and organizational controls				
b. Policies				

**Table 8: Electro-Optical and Communication Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	EO 2710	EO 2750	EO 3750	CM 3112
c. Personnel				
d. Physical and environmental security				
e. Computer operations				
f. Contingency planning				
5. Components of EDP security: technical				
a. Communication and electronic exposures	+			
b. Hardware	+			
c. Encryption	+			
d. Software	+			
B. Organizational and Administrative Controls				
1. Trade secrets, employee agreements, conflict of interest				
2. Security policy				
a. Intent (related to sensitivity)				+
b. Access to and distribution of information				
c. Laws				
d. Regulations				
e. Company policy				
f. Mandatory and discretionary security				
g. Accountability: identification, authentication, audit				
3. Responsibility areas, System Security Officer				

**Table 8: Electro-Optical and Communication Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	EO 2710	EO 2750	EO 3750	CM 3112
a. Basic role				
b. Duties				
c. Training and skills for a System Security Office				
4. Employee training				
a. Orientation				
b. Skills				
5. Telecommuting				+
C. Personnel Consideration				
1. Human motives for criminal action				+
2. Employee selection				
a. Application forms				
b. Permissions for investigations				
c. Security clearance and citizenship				
3. Professional certificates				
4. Working environment				
a. Vacations and job rotation				
b. Employee-management relations				
c. Career path planning				
d. Remuneration				

**Table 8: Electro-Optical and Communication Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	EO 2710	EO 2750	EO 3750	CM 3112
5. Access rights and privileges				
6. Prosecution for adverse actions				
7. Employee separation				
D. Physical and Environmental Security				
1. Site location and construction				
a. Computer room considerations				
b. Special microcomputer problems				
2. Physical access				
a. Access vs. security				
b. Rooms, windows, doors, keys				
3. Power				
a. Spikes, surges, brownouts				
b. Costs of prevention/protection equipment				
4. Air-conditioning				
5. Water exposures and problems				
6. Fire prevention				
7. Fire protection				
8. Tape and media libraries; retention policies				
9. Waste disposal				
10. Off-site storage				



**Table 8: Electro-Optical and Communication Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	EO 2710	EO 2750	EO 3750	CM 3112
11. Document libraries and controls				
<b>E. Computer Operations</b>				
1. Organization of computer operations				
a. Mainframes				
b. Minicomputers				
c. Microcomputers/office automation				
2. Separation of duties				
3. Controls at interfaces				
4. Media controls				
5. Backup procedures				
6. People controls				
<b>F. Contingency Planning</b>				
1. Backups and procedures				
a. Data				
b. Manuals and documentation				
c. Equipment				
1. Air conditioning				
2. Uninterruptible power supply				
2. Catastrophe planning				

**Table 8: Electro-Optical and Communication Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	EO 2710	EO 2750	EO 3750	CM 3112
a. Stages in a disaster				
b. Planning and response teams				
c. Testing plan				
d. Communication of plan				
3. Security and controls in off-site backup and facilities				
4. Business and DP insurance				
5. Software escrow arrangements				
<b>IV. Safeguards: Security and Control Measures, Technical</b>				
A. Hackers and reality: Perception of Risk				
B. Communications and Electronic Exposures				
1. Locus of attack				
a. Terminals	+			+
b. Hosts	+			+
c. Front-end processors	+			+
d. Gate ways	+			+
e. Links	+			+
f. Switches (multiplexors, packet switching, etc.)	+			+
g. Special problems with intelligent workstations	+			+
2. Types of attack				
a. Passive: disclosure; traffic analysis; add/remove nodes	+			+

**Table 8: Electro-Optical and Communication Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES		EO 2710	EO 2750	EO 3750	CM 312
b.	Active: modification; insertion; deletion; replay	+			+
3.	Electronic				
a.	Incoming: interruptions; static; FRI; EMP	+			+
b.	Outgoing: leakage	+			+
c.	Solutions: shielding	+			+
4.	Communications				
a.	Value-added communications	+			+
b.	exposures incoming: noise and interference	+			+
c.	Exposures outgoing: interception, replacement	+			+
d.	Solution: physical measures	+			+
e.	Solutions: encryption	+			+
f.	ISO OSI communications standards	+			+
5.	Network design				
a.	Design considerations				
1.	Integration of countermeasures into network				+
	design: cryptographic checksum; time stamp;				
	Bell/LaPadula model				
2.	Integration of countermeasures into protocol layers:				+
	link level encryption; end-to-end encryption				

**Table 8: Electro-Optical and Communication Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	EO 2710	EO 2750	EO 3750	CM 3112
b. Assurance				
1. Concept of trust				
2. Degrees of trustworthiness				
3. Trusted network base				
4. Testing				
5. Formal specification				
6. Formal verification				
C. Encryption				
1. Definition (plaintext, ciphertext; encryption/decryption)	+			
2. Public key and private key	+			+
3. Key distribution	+			+
4. Link level, end-to-end	+			+
5. Block mode, cipher block chaining, stream ciphers	+			+
(synchronous and self-synchronous)				
6. DES, RSA	+			+
7. Cryptanalysis and strength of cipher (theoretically secure	+			
computationally secure)				
8. Advantages and disadvantages	+			
D. Software and Operating System Controls				
1. Secure operating systems				

**Table 8: Electro-Optical and Communication Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	EO 2710	EO 2750	EO 3750	CM 3112
a. History				
b. Concepts: capabilities, reference validations				
1. Secure kernels				
2. Reference validations and capabilities				
c. Present guidelines and standards, trusted computer base				
d. Design principles fro secure systems				
1. Least privilege				
2. Open design				
3. Fail-safe defaults				
4. Economy of mechanisms				
5. Naturalness (human factors)				
6. Continuous protection				
e. Common penetration methods and countermeasures				
1. Trojan horse; virus; worm; salami; piggyback;				
deception; human compromise; etc.				
2. Controls on changes; audit trails; program library;				
code comparision; checksums and encryption;				
vaccines and antiviral agents; access control; etc.				
2. Access control				

**Table 8: Electro-Optical and Communication Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	EO 2710	EO 2750	EO 3750	CM 3112
a. Discretionary access control				
1. Subjects and objects				
2. Access privileges				
3. Granting/revoking of privileges				
4. Access control lists				
5. Capabilities, descriptors				
6. Supervisor states, rings, domains				
b. Non-discretionary access control				
1. Labels on subjects, objects				
2. Rules for reading, writing				
3. Software Controls: Development				
a. The real problem: bugs				
b. Software engineering principles: layering, modularity				
c. Structured methods				
d. Formal specification and verification				
e. Program library/librarian				
f. Data dictionary as a control				
g. Conversion and implementation				
4. Software controls: Maintenance				
a. Separation of duties				

**Table 8: Electro-Optical and Communication Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	EO 2710	EO 2750	EO 3750	CM 3112
b. Testing controls				
c. Change control				
5. Assurance				
a. Integrity				
b. Testing				
c. Specification/verification				
d. Facility management				
e. Disaster/contingency				
f. Compliance/degree of trust				
E. Database systems security				
1. Overview				
a. Review of basic concepts of information protection				
b. Role of information protection in database systems				
2. Threats				
a. Direct disclosure of data				
b. Modification of data/tampering with data				
c. Inference				
d. Aggregation				
e. Trojan horse				

**Table 8: Electro-Optical and Communication Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	EO 2710	EO 2750	EO 3750	CM 3112
f. Covert disclosure of data				
3. Policy/mechanism				
a. Policy versus mechanism				
b. Access controls				
1. Access right and privileges				
2. Access control policies				
3. Granularity				
4. Labels				
5. Access control mechanisms				
c. Inference controls				
d. Integrity controls				
1. Integrity policy				
2. Integrity mechanisms				
e. Accountability controls				
1. Identification and authentication				
2. Audit				
4. Design issues				
a. Protection Approaches				
1. Trusted kernel				
2. Trusted filter				



**Table 8: Electro-Optical and Communication Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	EO 2710	EO 2750	EO 3750	CM 3112
3. Encryption				
b. Performance				
c. Storage				
d. Access control vs. integrity				
e. Assurance				
<b>V. Legal Environment and Professionalism</b>				
A. Law and legislation				
1. The underlying problem				
a. Theft, copying software, privacy				
b. Fraud				
c. Physical abuse				
d. Misuse of information				
e. Sabotage				
2. Laws as tools for computer security				
a. Privacy laws and legislation				
b. Intellectual property laws				
1. Copyright law				
2. Trade secret law				
3. Patent law				

**Table 8: Electro-Optical and Communication Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	EO 2710	EO 2750	EO 3750	CM 3112
4. Trademark law				
c. Federal laws (esp. Computer Security Act 1987)				
d. State statutes				
e. DPMA Model Computer Crime Bill				
f. Computer crime legislation in other countries				
3. Legislation as legal options to control computer crime				
a. License agreements (consumer license agreements)				
b. permanent license agreements				
c. Intellectual property rights				
d. Employee non-disclosure considerations				
e. Contracts				
1. Software development contracts				
2. Legal aspects of software purchasing				
3. Leasing contracts				
f. Warranties for software and hardware				
4. Control of strategic materials				
5. Fraud and crime prevention and detection				
6. Investigation; evidentiary trial				
B. Ethics and professionalism				
1. Ethical decision-making				

**Table 8: Electro-Optical and Communication Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	EO 2710	EO 2750	EO 3750	CM 3112
2. Professional societies				
a. British Computer Society				
b. North America: DPMA and ICCP				
c. Canada: CIPS and DPMA				
1. CIPS				
2. DPMA Canada				
d. Computer Professionals for Social Responsibility				
e. EDP Auditors Foundation				
3. National Computer Security Center				
4. National Bureau of Standards				
5. Certificate in Data Processing(CPC); Certified Information Systems Auditor(CISA)				
<b>VI. CICA Computer Control Guidelines</b>				
A. Accounting and auditing				
1. Computer Control Guidelines				
a. Responsibility for Control				
b. Information Systems Development and Acquisition				
c. Information Systems Processing				
d. Segregation of Incompatible Functions and Controls				

**Table 8: Electro-Optical and Communication Courses**

COMPUTER SECURITY CONCEPTS AND ISSUES	EO 2710	EO 2750	EO 3750	CM 3112
e. Application Controls				
2. Information systems audit				
a. Security review objectives				
b. Specific security controls				
c. Security review process				
d. Evidence accumulation				
e. Evaluation of test results				
f. Communication of control weaknesses				

## LIST OF REFERENCES

- [ Ref. 1 ] Stoll, C. *The Cuckoo's Egg*, Doubleday, 1989.
- [ Ref. 2 ] Computer Science Department, Purdue University, Technical Report Number CSD-TR-823, *The Internet Worm Program: An Analysis*, by E. H. Spafford, pp. 1-2, 1988.
- [ Ref. 3 ] U.S. General Accounting Office Report, GAO / T-IMTEC-92-5, *Hackers Penetrate DoD Computer Systems*, by J. L. Brock, pp. 2-3, 1991.
- [ Ref. 4 ] Baker, Richard H., *Computer Security Handbook, 2nd Edition*, pp. xvii-xviii, TAB Professional and Reference Books, 1991.
- [ Ref. 5 ] Denning, Peter J., ed., *Computers Under Attack: Intruders, Worms, and Viruses*, p. xiv, ACM Press/Addison-Wesley, 1990.
- [ Ref. 6 ] Russell, D., and Gangemi Sr., G. T., *Computer Security Basics*, pp. 8-11, O'Reilly and Associates, Inc., 1991.
- [ Ref. 7 ] Ibid.
- [ Ref. 8 ] Ibid., 17.
- [ Ref. 9 ] Ibid., 13.
- [ Ref. 10 ] Denning, iii.
- [ Ref. 11 ] Ibid., 456.
- [ Ref. 12 ] Ibid., 459-460.
- [ Ref. 13 ] Brock, 5.

- [ Ref. 14 ] Interview between J. Zucker, Lieutenant Commander, USN, Moffett Naval Air Station, Mountain View, CA, and the author, 25 November, 1991.
- [ Ref. 15 ] Interview between D. Hutton, ADP Manager, Naval Postgraduate School, Monterey, CA, and the author, 15 November, 1991.
- [ Ref. 16 ] Russell, 283.
- [ Ref. 17 ] Ibid., 104.
- [ Ref. 18 ] Ibid.
- [ Ref. 19 ] Ibid., 112.
- [ Ref. 20 ] Fites, P.E., "Professional Certification for Information Systems Security Practitioners", *Computer Security Journal*, v. V, n. 2, pp. 75-88., Computer Security Institute, 1990.
- [ Ref. 21 ] Ibid., 76.
- [ Ref. 22 ] Ibid., 77.

## INITIAL DISTRIBUTION LIST

Defense Technical Information Center Cameron Station Alexandria, VA 22304-6145	2
Dudley Knox Library Code 52 Naval Postgraduate School Monterey, CA 93943-5002	2
Chairman, Code 37 Administrative Sciences Department Naval Postgraduate School Monterey, CA 93943	2
Administrative Sciences Department Code AS/Bd Naval Postgraduate School Monterey, CA 93943	1
Computer Science Department Code CS/Sp Naval Postgraduate School Monterey, CA 93943	1
Commander Naval Computer and Telecommunications Command 4401 Massachusetts Ave., N.W. Washington, D.C. 20394-5000	1
Director of Space and C4 System Requirements N6(OP 094) Office of the Chief of Naval Operations Washington, D.C. 20370-5000	1

**CDR Debbie Campbell** 1  
**National Computer Security Center NSA / C81 / APSXI**  
**9800 Savage Rd.,**  
**Ft. Meade, MD 20755-6000**

**Naval Information Systems Management Center** 1  
**Bldg. 166,**  
**Washington, D.C. 20374-5070**

**SPAWAR** 1  
**Code 2241**  
**Crystal City SCPK, 700**  
**Washington, D.C. 20363-5100**