DRAFT

INTEGRATING INFORMATION SECURITY

PUBLICATION 0002D

NATIONAL INFORMATION ASSURANCE
TRAINING AND EDUCATION CENER
IDAHO STATE UNIVERSITY
Director Corey D. Schou, PhD, CISSP
Professor, Information Systems
Associate Director, James Frost, PhD
Assistant Professor, Information Systems

Derived from Simplot Decision Support Center Report 162

By
Corey D. Schou, PhD
James Frost, PhD
Nathan Wingert

With
Jason Larsen
Herbert LaFond, Edward Munson

TABLE OF CONTENTS

PREFACE

Information is an organizational resource. Security of this resource within an organization is important. Frequently, the management of the organization does not take an active role in the protection of this resource nor do they understand the concept of trusted systems. The absence of active participation is sometimes based on ignorance of the actual value of the resource.

To overcome this ignorance, the education of leaders must be improved. This is an outline of information security course materials to be used, primarily, in a non-technical curriculum. The following paragraphs provide some of the critical social focus for this course.

Near the beginning of the American experiment, one patriot said, “I have but one lamp by which my feet are guided and that is the lamp of experience. I have no way of judging of the future but by the past.” How are we to avoid the pitfalls of the future in our Information Society or as participants in the Information Revolution? These terms describe extensions of the industrial revolution that has been molding the American Experiment for the last 200 years.

About one hundred fifty years ago Charles Dickens, in his novel Hard Times (1845), detailed the impact of some of the social and economic conditions being created by the industrial revolution. Dickens describes the dehumanization of the worker during this period of social upheaval and economic change. He shows the effects of management reacting to the workers as replaceable pieces or cogs of the physical system that they use to create their products. Management was not able, or willing, view these cogs as individuals. This is the first flicker of light in the lamp of experience.

In the last fifty years, we have seen the beginnings of a new industrial revolution. The Blue Collar worker initially welcomed job aids that increased his productivity and reduced his workload by adding a mechanical assist to his efforts. In many cases we have seen the typical Blue Collar worker replaced by an Iron Collar worker - automated assembly process or the robot. Since the Iron Collar worker neither bargains for wages, calls in sick, nor needs an endowed retirement program; this Iron Collar worker improves the bottom line performance and therefore is judged to be good for business.

When the human problems associated with the introduction of the Iron Collar worker are examined, we are given further justification by referring to the relief from repetitive tasks and the attendant quality of life improvement for the workers. This change is fine for those who still maintain their jobs or are able to be retrained; however, some individuals are not able to make the transition comfortably if at all. One should not call a halt to this progress; rather, managers should be educated to deal with the long range economic and human impact of their decisions while examining the bottom line.

Remembering Hard Times is important for the next generation since we are about to embark on a new series of socio-industrial changes. While Iron Collar workers spread throughout the industrial work place, the computer resource is spreading to the middle management class of the corporation. Currently the White Collar work force views the computer as a benign tool that supports his decision making process, reduces his workload and assists his intellectual efforts.

In the near future we may well see portions of the White Collar work force supplanted by the Silicon Collar worker - the computer and its associated support humans. The Silicon Collar worker is ideally suited for repetitive programmable decisions and actions and the attendant minimization of decisions at risk and uncertainty is a goal sought by management. The Silicon Collar worker needs neither stock options, Christmas bonuses, nor retirement plans. This Silicon Collar worker will impact the middle management class and their routine decision making more directly than any other change in this century and initially it will be more susceptible to being undermined by modern Luddites and saboteurs.

There is a chance we are beginning to see these modern Luddites already. Several years ago, James L. McKenney, through a series of articles in the Harvard Business Review talked about the existence of an information archipelago. The author specifies three islands – data processing, telecommunications and word processing. The archipelago he describes and its attendant bridges is critical to most computing and information related activities in the modern business. The bridges (networks) are critical to the success of the modern Silicon Collar Worker in that they carry the lifeblood - data.

Clifford Stoll in his recent book, *The Cuckoo's Egg*, describes the deep personal anger he felt when he discovered that someone was prying at the door of his computer and violating his privacy. This modern Luddite was breaking down the fabric of the network - the threads of trust that hold an information society together.

As practitioners and leaders in the field, we have input to the next generation and the institutions that educate them. Perhaps we should insist that in addition to the traditional technical subject areas in engineering, computer science and information systems, course material should include ethics, security and privacy, and perhaps even a bit or two on social and economic issues be included. We should see that these issues are not be relegated to the foundation courses of our academic institutions but should be woven into the intellectual fabric throughout the curriculum. Should we fail to do this weaving, the next generation may enter the latest phase of the industrial revolution ill equipped to deal with the broader issues that will confront them.

As we enter this new era, we should not forget that systems and networks are not made of printed circuit boards nor of wires nor of bits and pieces – they are made of people - individuals. Should we forget this we may perhaps develop a new Hard Times for a modern day Dickens to write about.

INTRODUCTION

To manage is to plan for, allocate and conserve resources. Information is a resource. It has the same characteristics of cost, value, and scarcity, as do the more familiar material, financial and human resources. The use of computers has provided a means to exploit the potential value of information a manner never before possible. It is easy to explain to management why other resources need protection; however, the information resource is frequently overlooked or is the 'stepchild'.

These course materials are designed to train managers to instruct the organization to

1) understand the resource - know thoroughly the nature and characteristics of the resource, including its potential and limitations;
2) maintain and conserve the resource - acquire, maintain, and conserve the quantity and quality of the resource needed by the organization;
3) exploit the resource - Develop the potential of the resource and exploit the potential to the fullest possible extent to meet the needs of the organization;
4) employ the resource - effectively and efficiently apply the resource to the activities of the organization; and
5) integrate the resource - effectively coordinate the use of the resource with the use of other resources to bring efficiently a desired result.

while providing adequate security for the resource.

To implement this curriculum, a series of eight modules dealing with information security was created. Each of the modules is designed to be an addition to existing courses in a business or information systems curriculum. In addition, segments of the modules may be combined to create specialized courses on information security. Figure one shows the relationship of the modules within the series. Level One courses are intended for the lower division students while Level Two and Three are for Juniors and Seniors respectively. There is a capstone course, Corporate Security Management, which summarizes many components of all other courses. For Accounting students, the module Introduction to Accounting Controls and EDP Auditing many function as a capstone course.

The reader should be aware that there is planned redundancy among the modules since one cannot plan for the actual implementation of these modules within a curriculum.

Module one (Introduction to Information Protection) is an introduction to information protection principles and provides basic security concepts for undergraduate general business majors and students enrolled in an introductory information systems course. Each major issue presented in this module is detailed further in its own module that can be supplemental to courses throughout a business and information systems curriculum. This module is designed to be used as part of a freshman or sophomore level Management Information Systems course, such as the recommended DPMA course CIS/86-1, (Introduction to Computer Information Systems.)

Module two (PC/Workstation Security) introduces essential concepts of personal information security and outlines components of an introductory course dealing with the basic security concepts of information processing. This module contains the fundamental knowledge for subsequent modules in this series and is intended to be supplemental to introductory courses in curricula for computers or information systems. Topics include ethics and professionalism, security and data control, computer room environment, PC/workstation security familiarization, and physical security.

Module three (Security Fundamentals) is introductory in nature and provides basic security concepts for undergraduate general business majors and specialized Information Systems Majors. This module outlines and describes the basic requirements for planning, organizing and managing security in an organization. Topics include personal and organizational ethics; hardware and software issues; security and threats to data; recovery, control and audit procedures; and corporate security costs and benefit identification. A bibliography and selected case studies are provided and may be used at the discretion of the instructor to expand any of these topics. This module might be included as part of a Junior level management information systems course or integrated as part of other business courses.

Module four (Information Security Law and Legislation) may be used in both Information Systems courses, as well as courses in the common body of knowledge, as defined by the American Assembly of Colleges and Schools of Business (AACSB). This module is intended to be part of a junior or senior level course in a Management Information Systems curriculum that covers the management aspects of information systems. For example, it might be included as a module in the DPMA Model Curriculum for Undergraduate Computer Information Systems courses CIS/86-18 (Information Resource Planning and Management) or CIS/86-14 (Computer Control and Audit). It also could be included as part of MIS or Legal Environment courses.

Module five (System Security) is the first of the senior level modules and addresses mainframe security considerations. The module defines advanced requirements for security and the criteria on which satisfaction of those requirements can be judged. Hardware, software, firmware, and procedures are considered as mechanisms to protect appropriately a system. The described process starts by defining the sensitivity of a system and proceeds through establishing criteria and evaluating the degree to which the criteria are met.

This module is intended to be used as part of a course in Systems Design and Development, System Management, or as an information security course. It may be taught either as an integrated part of instruction on the systems development life cycle or as a separate module. This module may be included in the DPMA Model Curriculum in CIS/86-14 (Computer Control and Audit) or CIS/86-18 (Information Resource Planning and Management).

Module six (Communications Security) is intended to be included in an undergraduate course on data communications and networking for information systems and business majors. Several perspectives could be chosen as the basis for this module: an example might be, a detailed technical perspective for students who are interested in designing data communication systems and networks.

However, this module is written from a management perspective for those students who want to become intelligent users of such systems or those who aspire to a management role in an organization that relies on data communications systems or networks to interconnect elements of its information processing systems, either internally or externally.

The module is designed to be added to an existing data communications course, or it could be added to a course in office automation. If the institution is using the DPMA Model Curriculum for undergraduate Computer Information Systems, then it could be added to CIS/86-15, (Distributed Intelligence and Communication Systems).

Module seven (Corporate Security Management) deals with top management and policy considerations. Responsibilities of managers vary, depending on their level in an organization, and this module introduces differences in responsibilities at various levels of management. The role of the System Security Officer (in organizations large enough to warrant a SSO) is discussed.

A corporate security management plan needs the involvement of all levels of management to ensure that the program is properly and thoroughly implemented. The program should clearly identify local, state, and federal legislation that defines responsibility to ensure that all members of the corporation understand and are able to implement a specified plan. Ultimately, the corporation is held responsible for the accuracy and integrity of corporate data.

This module is intended to be included as part of a course, such as the CIS/86-18 (Information Resource Planning and Management). Other courses, such as those specialized in security or data processing management concepts, might include this material, at least in outline. A Business Policy course that has a significant MIS component, could benefit from including this module as a case study or as part of examining the responsibilities of senior management to interact with the external environment.

Module eight (Introduction to accounting and auditing controls) is an introduction to accounting and auditing controls concepts intended for a broad variety of students in courses where an appreciation of such concepts is needed. The module outlines key accounting and auditing concepts and describes the various roles played by management, information systems professionals, internal auditors, and external auditors. It deals with management control, application control, evidence gathering and evaluation, and management of the EDP audit function. The module may be used in junior or senior level information systems courses or integrated in other business courses.

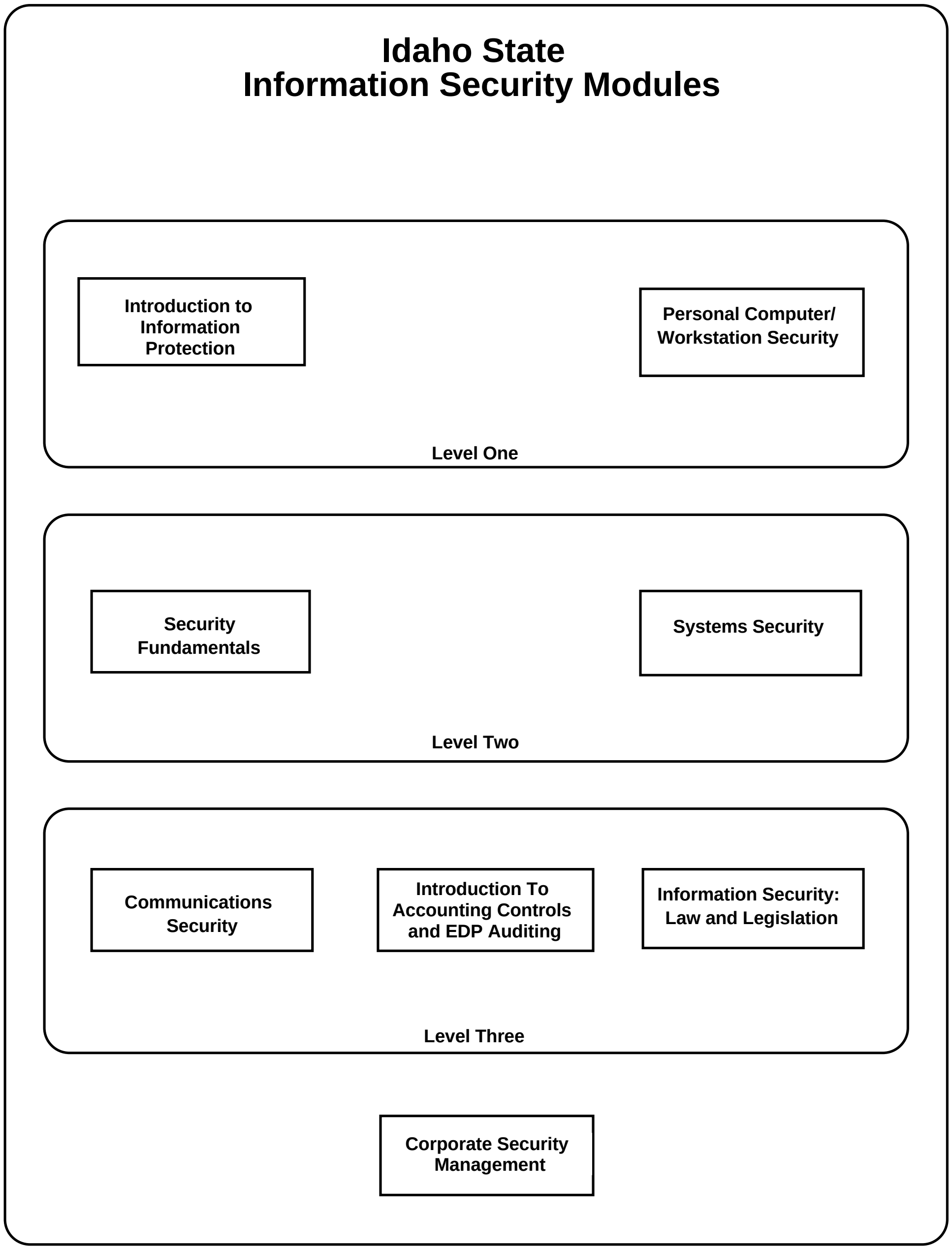


Figure 1 Curriculum Outline

HISTORY

These modules evolved from a workshop, sponsored by the Department of Defense and hosted by Idaho State University, held in June 1988 at Pocatello, Idaho. The workshop was conducted to develop appropriate information security modules suitable for integration into undergraduate curricula in colleges of business and also information systems programs.

The participants identified appropriate modules and produced module outlines that were then expanded and annotated. The modules identified include: Introduction to Information Protection, PC/Workstation Security, Security Fundamentals, Information Security Laws and Legislation, System Security, Communications Security, and Corporate Security Management.

Subsequently a module, Introduction to Accounting and Auditing Controls by Terry L. Campbell The Pennsylvania State University, Suzanne M. Spitzer Spectrum Consulting and Annette Moore, Idaho State University. Philip Fites contributed to the creation of the question bank that accompanies the modules. These questions draw heavily on his book *Control and Security of Computer Information Systems* published by W. H. Freeman/Computer Science Press. Jim Frost, Idaho State University, compiled the overhead projection materials.

There is a separate module on ethics (John Kilpatrick, Idaho State University, Donald Madden LMA Video)/

Additional materials may be available from:

Corey D. Schou, Ph.D.
Chairman, Computer Information Systems
Idaho State University
P.O. Box 4043
Pocatello, Idaho
83205

INTRODUCTION
TO
INFORMATION PROTECTION

Revised August 1990
Revised May 1995
Revised February 2001

National Information Assurance Training and Education Center
College of Business
Idaho State University

Description:

This introductory module provides basic security concepts for undergraduate general business majors and students enrolled in an introductory information systems course. Each major issue presented in this module is detailed further in its own module, which can be supplemental to courses throughout the business and information systems curriculum. This module is designed to be used as part of a freshman or sophomore level Management Information Systems course, such as the recommended DPMA course CIS 86-1 (Introduction to Computer Information Systems).

INTRODUCTION TO INFORMATION PROTECTION

OBJECTIVES:

The two primary objectives of this module are to:

- Introduce business and non-business majors to basic information security problems; and
- Identify the primary areas that deal with information security.

Upon successful completion of this module the student will understand basic information security problems and will be able to identify areas where additional study may be needed.

Following this module, the student would progress to PC/Workstation Security module or the Security Fundamentals module that lays the foundation for advanced study in systems security.

LEARNING OBJECTIVES

Upon completion of this module, the student should be able to:

- Understand the need for security in an organization;
- Identify basic security problems;
- Understand ethical issues involved with the use of information systems security; and
- Identify major areas in security management for additional study.

PREREQUISITES

No previous study or lab experience is assumed. The PC/Workstation module may be taken before, concurrently, or following this module.

Topic Outline

I. Information as a Corporate Resource
 A. Security As Part Of The Total Organization
 B. Understanding The Organization
 C. Identifying Sensitive Data
 D. Controlled Sharing Of Information And Resources

II. Basic Information Systems Security Problems
 A. Natural Disasters
 B. Accidental Problems
 C. Malicious Threat

III. Ethical Issues
 A. Responsible decision-making
 B. Confidentiality & Privacy
 C. Piracy
 D. Fraud & Misuse
 E. Liability
 F. Copyright
 G. Trade Secrets
 H. Sabotage

IV. Areas of Information Systems Security Study
 A. PC/Workstation Security
 B. Security Fundamentals
 C. Information Security Laws & Legislation
 D. System Security
 E. Communications Security
 F. Corporate Security Management

Annotated Outline

I. INFORMATION AS A CORPORATE RESOURCE

A. *Security as Part of The Total Organization*

Information security is not simply software or hardware security, and it does not stand apart from the total organization. An organization's policies, plans and procedures may affect security needs, and security practices may affect those policies, plans or procedures. The important point is that a secure system is integral to the total organization.

B. *Understanding The Organization*

If a secure system is part of the total organization, then one must understand the organization, its goals, objectives, policies and procedures. If the objectives of an organization are unclear, then implementing new technology will not help. If procedures are not secure, then new technology will not make them secure. Understanding the organization is the first step in planning for a secure system.

C. *Identifying Sensitive Data*

After establishing a clear understanding of the organization's function and how it is to complete its objectives, the first step in planning for and developing a secure system is to identify sensitive data. Recognize specific levels of security and that each may not be equally valuable. Identifying sensitive data and determining their value before the fact is a most difficult task for any organization. Unfortunately for most Management Information Systems (MIS) directors, management will more easily recognize the true value of data after the data have been disclosed to unauthorized individuals and are compromised.

D. *Controlled Sharing of Information and Resources*

Sharing of information and resources is increasingly possible through increased networking, communications and connectivity. As this data sharing increases, the problem of information security increases exponentially. The problem for management is one of encouraging increased productivity through technology while maintaining what will probably be an increasingly insecure system.

II. BASIC INFORMATION SYSTEMS SECURITY PROBLEMS

A. *Natural Disasters*

Natural disasters, such as floods, lightning, brown-outs, fire and earthquakes, are the most obvious security problems for most organizations. Since the source of these problems is generally uncontrollable, one must plan for the possibility. Physical location of computer systems, control of electrical surges or spikes and clean fire suppression methods are possible techniques to discuss when dealing with this topic. A pre-defined disaster plan, including appropriate off-site backup, helps to avoid regret.

B. *Accidental Problems*

Many threats to a system result from unintentional errors created either by a user or by the system itself. Examples include the accidental disclosure of data, inadvertent modification or destruction of data, faulty software that may produce incorrect data, residual data left in the system and that may contaminate new data, and wrong parameters that get passed inappropriately. The most common forms of accidental threats are employee mistakes. Ongoing training programs, both formal and informal, can help prevent many of these problems.

C. *Malicious Threats*

Malicious threats are deliberate attempts to circumvent or defeat the system's protection mechanisms, or exploit weaknesses in such mechanisms. A trapdoor is a "special element that when inserted in a program or system allows the intruder to bypass protective features safeguarding the secure functioning of a system." The Trojan horse technique of penetration "consists of supplying the computer with what is perceived appropriate and acceptable information, but in reality contains secret instructions for unauthorized behavior."

Users may tamper with data or programs, snoop or browse through a system or intentionally disclose data. A worm or virus may be inserted in a program and spread throughout the system. Malicious threats are the most difficult type of security problem to deal with. They may start from within or outside the organization.

III. ETHICAL ISSUES

The foundations of all secure systems are the moral principles and practices and the professional standards of all employees of the organization, i.e., while people are part of the solution, they are also most of the problem. The following issues are examples of security problems which an organization may have to deal with:

A. *Ethics and Responsible Decision-Making*

The foundation of all security systems is formed by moral principles and practices of those people involved and the standards of the profession. That is, while people are part of the solution, they are also most the problem. Security problems with which an organization may have to deal include: responsible decision-making, confidentiality, privacy, piracy, fraud & misuse, liability, copyright, trade secrets, and sabotage. It is easy to sensationalize these topics with real horror stories; it is more difficult to deal with the underlying ethical issues involved.

The student should be made aware of his individual responsibility in making ethical decisions associated with information security.

B *Confidentiality & Privacy*

Computers can be used symbolically to intimidate, deceive or defraud victims. Attorneys, government agencies and businesses increasingly use mounds of computer generated data quite legally to confound their audiences. Criminals also find useful phony invoices, bills and checks generated by the computer. The computer lends an ideal cloak for carrying out criminal acts by imparting a clean quality to the crime.

The computer has made the invasion of our privacy a great deal easier and potentially more dangerous than before the advent of the computer. A wide range of data are collected and stored in computerized files related to individuals. These files hold banking information, credit information, organizational fund raising, opinion polls, shop at home services, driver license data, arrest records and medical records. The potential threats to privacy include the improper commercial use of computerized data, breaches of confidentiality by releasing confidential data to third parties, and the release of records to governmental agencies for investigative purposes.

The basic law that protects our privacy is the Fourth Amendment to the United States Constitution, which mandates that people have a right to be secure in homes and against unreasonable search and seizure. In addition, many laws have been enacted to protect the individual from having damaging information stored in computerized databases.

C. *Piracy*

Microcomputer software presents a particular problem since many individuals are involved in the use of this software. Section 117 of the copyright laws, specifically the 1980 amendment, deals with a law that addresses the problem of backup copies of software. This section states that users have the right to create backup copies of their software. That is, users may legally create a backup copy of software if it is to be held in archive. Many software companies provide a free backup copy to users that precludes the need for to users purchase software intended to defeat copy protection systems and subsequently create copies of their software. If the software purchased is actually leased, you may in fact not even be able to make backup copies of the software. The distinction between leasing and buying is contained within the software documentation. The copyright statement is also contained in the software documentation. The copyright laws regarding leased material state that the leasor may say what the leaseholder can and cannot do with the software. So it is entirely up to the owner of the software as to whether or not users may make backup copies of the software. At a time when federal laws relating to copyright protection are evolving, several states are considering legislation that would bar unauthorized duplication of software.

The software industry is prepared to do battle against software piracy. The courts are dealing with an increasing number of lawsuits concerning the protection of software. Large software publishers have established the Software Protection Fund to raise between $500,000 and $1 million to promote anti-piracy sentiment and to develop additional protection devices.

D. *Fraud & Misuse*

The computer can create a unique environment in which unauthorized activities can occur. Crimes in this category have many traditional names including theft, fraud, embezzlement, extortion, etc. Computer related fraud includes the introduction of fraudulent records into a computer system, theft of money by electronic means, theft of financial instruments, theft of services, and theft of valuable data.

E. *Liability*

Under the UCC, an express warranty is an affirmation or promise of product quality to the buyer and becomes a part of the basis of the bargain. Promises and affirmations made by the software developer to the user about the nature and quality of the program can also be classified as an express warranty. Programmers or retailers possess the right to define express warranties. Thus, they have to be realistic when they state any claims and predictions about the capabilities, quality and nature of their software or hardware. They should consider the legal aspects of their affirmative promises, their product demonstrations, and their product description. Every word they say may be as legally effective as though stated in writing. Thus, to protect against liability, all agreements should be in writing. A disclaimer of express warranties can free a supplier from being held responsible for any informal, hypothetical statements or predictions made during the negotiation stages.

Implied warranties are also defined by the UCC. These are warranties that are provided automatically in every sale. These warranties need not be in writing nor do they need to be verbally stated. They insure that good title will pass to the buyer, that the product is fit for the purpose sold, and that it is fit for the ordinary purposes for which similar goods are used (merchantability)..

F. *Patent and Copyright Law*

A patent can protect the unique and secret aspect of an idea. It is very difficult to obtain a patent compared to a copyright (please see discussion below). With computer software, complete disclosure is required; the patent holder must disclose the complete details of a program to allow a skilled programmer to build the program. Moreover, a United States software patent will be unenforceable in most other countries.

Copyright law provides a very significant legal tool for use in protecting computer software, both before a security breach and certainly after a security breach. This type of breach could deal with misappropriation of data, computer programs, documentation, or similar material. For this reason the information security specialist will want to be familiar with basic concepts of to copyright law.

The United States, United Kingdom, Australia, and other countries have now amended or revised their copyright legislation to provide explicit laws to protect computer program. Copyright law in the United States is governed by the Copyright Act of 1976 that preempted the field from the states. Formerly, the United States had a dual state and federal system. In other countries, such as Canada, the courts have held that the un-revised Copyright Act is broad enough to protect computer programs. In many of these countries the reform of copyright law is actively underway.

G. *Trade Secrets*

A trade secret protects something of value and usefulness. This law protects the unique and secret aspects of ideas, known only to the discoverer or his confidants. Once disclosed the trade secret is lost as such and can only be protected under one of the following laws. The application of trade secret law is very important in the computer field, where even a slight head start in the development of software or hardware can provide a significant competitive advantage.

H. *Sabotage*

The computer can be the object of attack in computer crimes such as the unauthorized use of computer facilities, alternation or destruction of information, data file sabotage and vandalism against a computer system. Computers have been shot, stabbed, short-circuited and bombed.

It is easy to sensationalize these topics with real horror stories; it is more difficult to deal with the underlying ethical issues involved.

IV. AREAS OF INFORMATION SYSTEMS SECURITY STUDY

Students may be introduced to several major areas of study. Each area listed in the topic outline is elaborated on as a separate module in this document. The purpose of this introductory module is to help students recognize some security problems inherent with each of the major areas of study and to encourage them to learn more about information security throughout their undergraduate program.

A. *PC/Workstation Security*
Students are introduced to basic ethical issues associated with using PC's, environmental and physical considerations for security, data integrity, and security training concepts. The PC/Workstation module may be used before, concurrently, or immediately following the "Introduction To Information Protection" module.

B. *Security Fundamentals*
The Security Fundamentals module, following the "Introduction To Information Protection" and "PC/Workstation" modules, lays the foundation for specialized advanced study about systems security that is covered in subsequent modules. An important aspect of this module is its emphasis on understanding the need for data security within an organization and the integration of a security program as part of the basic corporate goals, policies and procedures. Personal and corporate ethical issues are discussed.

C. *Information Security Laws and Legislation*
This topic should start with a discussion of underlying problems, such as information theft, privacy and fraud, and leads to the security laws and legislation that continue to evolve. Students review state and federal legislation and contracts associated with information security and crime. An important objective is for students to have a "general working understanding of the inter-relationship between various areas of law and security system design."

D. *System Security*
This module primarily addresses mainframe security considerations and goes into great detail about:

- System criticality, or the affect upon the organization if the system were to become unavailable
- System sensitivity, and the extent to which it is important to protect the system and
- Security policy, accountability and assurance.

E. *Communications Security*
A basic understanding of networking, communications and connectivity is helpful when dealing with communications security. The objective of this module is to investigate data protection in data communications systems and networks from a management perspective. This area of study is vital because of the increasing connectivity between PC's, workstations, minicomputers and mainframe computers, whether within a room, building or around the world. As the integration of hardware continues, the threat to data and information assets and resources grows rapidly. A description of protection mechanisms and countermeasures to these threats is included, plus cost/benefit tradeoffs are considered.

F. *Corporate Security Management*
This is the capstone module in this series of undergraduate teaching modules about information security. The focus is upon the need for a corporate security program and the responsibilities of managers at different levels within the organization. Risk analysis and contingency planning are discussed. A primary objective is the development of a corporate security management plan.

Teaching Considerations

A. Suggested Schedule:

The following sample module plan is based on the offering of one to three hours of lectures.

1. **Information as a corporate resource ....0.2 to 0.5 hours**
2. **Basic Security Problems.. 0.5 to 1.0 hour**
3. **Ethical Issues.. 0.3 to 1.0 hour**
4. **Major Areas of Information Systems Study .... 0.5 to 1.0 hour**

B. Class and Homework Exercises:

Following are examples of possible class/paper exercises that might enhance the lecture material for the module.:

- Find/report on current data security and computer crime problems. Use current journals and newspapers. What comes closest to your community; to you?
- Choose one ethical issue. Discuss it from the standpoint of
  - an organization,
  - an individual, and
  - the government.
- List six major areas of information security study and for each one, give three reasons why it is important.

Bibliography

Schou, C.D., Fites, P.E., & Burgess, J.D., "Corporate Security Management," in Information Security Modules, Department of Defense, 1989.

Consider this the capstone security module in this document. Emphasis is on the management of a corporate level data security program.

Denning, D.E., *Cryptography and Data Security*, Addison-Wesley, 1983.

Presently this is one of the principal textbooks in computer security. Good as a background reference.

Walston, C.E., "Communications Security," in *Information Security Modules*, Department of Defense, 1989.

Whiteside, T., *Computer Capers*, Mentor, 1978.

The problem of data security to our attention through many vignettes of some early "tales of electronic thievery, embezzlement, and fraud." Whiteside's stories can be used with reports of current problems, for example from *The Wall Street Journal* or *Fortune* magazine.

Johnson, Douglas W., *Computer Ethics: A Guide for the New Age*, The Brethren Press, 1984.

This low-cost, readable paperback book introduces critical issues, including: personal data, decision-making and identifying, building and maintaining ethics in a computer society. This book addresses the question of ethics in the indiscriminate use of the personal computer. The concept of what ethics are is proposed and suggestions are made for establishing a code for personal computer use.

Computer Professionals for Social Responsibility, Inc., P.O. Box 717, Palo Alto, CA 94301, 415/322-3778.

CPSR is an organization for computer professionals concerned about social issues. There are active chapters around the world. They produce a newsletter.

Mandell, Steven L., *Computer Data Processing, and the Law*, West Publishing Company, Minnesota, 1984.

This book has been designed especially for the functional aspects of data processing management.

Davis, G. G., *Software Protection, Practical and Legal Steps to Protect and Market Computer Programs*, Van Nostrand Reinhold, New York, 1985.

An academic discussion of intellectual property rights, copyright, unresolved problems with copyright, software warranties, export controls, and infringement remedies.

Burgess, J.D. & Watts, R.T., "PC/Workstation Security," in *Information Security Modules*, Department of Defense, 1989.

This module gives an introduction to security problems that one may have when working with a stand-alone PC or workstation (networked PCs or workstations are NOT considered here). This material is useful, for a one-person business as well as individual user who is part of a larger organization.

Richards, T., Schou, C.D. & Fites, P.E. "Information Systems Security Laws and Legislation," in *Information Security Modules*, Department of Defense, 1989.

Richards, et. al. review topics, timely laws and legislation about computer security as it relates to the individual and the organization.

Spiro, Bruce E. & Schou, Corey D., "System Security," in *Information Security Modules*, Department of Defense, 1988.

"Systems Security" is an upper level module that gives a detailed review of security issues and the integration of these details into an organizational security program.

PC/WORKSTATION SECURITY

Revised August 1990
Revised May 1995
Revised February 2001

National Information Assurance Training and Education Center
College of Business
Idaho State University

Description

This module introduces essential concepts of personal information security and outlines components of an introductory course dealing with the basic security concepts of information processing. This module contains the fundamental knowledge for subsequent modules in this series and is intended to be supplemental to introductory courses in curricula for computers or information systems. Topics include ethics and professionalism, security and data control, computer room environment, PC/workstation security familiarization, and physical security.

PC/WORKSTATION SECURITY

OBJECTIVES:

The objective of this module is to introduce the fundamental concepts of personal computer security.

LEARNING OBJECTIVES

Upon completion of this module, the student should be able to:

- understand the basic concepts of ethics associated with the use of a personal computer or workstation.
- identify factors associated with controlling the computer room environment.
- identify basic requirements for providing the physical security of personal computers and workstations.
- identify methods and techniques for providing the security and integrity of data.
- identify the need for security training.

PREREQUISITES:

NONE

This material is intended to be used in conjunction with an introduction to data processing course (including lab) such as the DPMA course CIS/86-1.

NOTE:

The term workstation as used in this module refers only to the function of the workstation as a stand alone device. There is no intention to include the added functions of the workstation in its specialized function to support engineering.

Topic Outline

I. Ethical Use of the Computer
II. Computer Room Environment
   A. Temperature
   B. Foreign Materials
   C. Radio Frequency Interference
   D. Power Surges or Brownouts
III. Physical Security
   A. Location and Construction
   B. Computer Room Access
   C. Physical Control
IV. Data Security
   A. Software Control
   B. Backup Procedures
   C. Recovery Techniques
   D. Data Encryption and Access Control
V. Security Training

Annotated Outline

I. ETHICAL USE OF THE COMPUTER

There are several ways of identifying and deciding ethical issues. One of the most common ways of categorizing these approaches is the rules vs. consequences criteria. The first argues that our actions should be guided by general rules or principles: do not harm; tell the truth; do not steal; respect for persons. The second argues that we should assess the "rightness" of an action or decision by the consequences that will likely result. Most commonly the second approach identifies some "value" or values, and measures the actions by the extent to which these values are or are not enhanced, or progress made toward certain goals, such as a better life for all.

On reflection is should be clear that there is no consensus about which of these is the more appropriate. In the ensuing discussion, arguments and positions will be presented using both of these approaches

The magnitude of computer use in our society dictates that ethical standards or guidelines be developed.

Any code of computer ethics should stipulate who monitors what is put into personal computers. Ethical guidelines are required for decisions of what data are allowable and legitimate for personal computers.

Students should understand that distributing unauthorized copies of a computer program it is theft. It is also wrong to break a security code to a bank, a school's grading system, or the telephone company.

Ethics relate to those who sell computer hardware and software, as well. Not all computer vendors deal adequately with the responsibilities associated with a sale. Very few, if any, supply sufficient training, service, education, and proper use of the computer.

The groups that need to be concerned about the development and teaching of ethics include users, suppliers and trainers in personal computers.

II. COMPUTER ROOM ENVIRONMENT

A. *Temperature*
While a personal computer is somewhat insensitive to its environment, some attention to the environment will prolong the life and increase the safety of data stored in the machine. A rule of thumb to apply when considering the physical environment is, "If you are comfortable, the computer is comfortable."

B. *Foreign Materials*
Establish and enforce firm, consistent policies regarding the presence of food, drink, smoke, and dust in the computer room.

C. *Radio Frequency Interference (RFI)*
All electronic equipment produce radiation and emanations of varying frequencies. Take care that the computer will operate in the environment that contains emanations from other electronic devices and that the computer will not interfere with other electronic devices.

If care is not taken, RFI may be received outside the computer facility and, by sophisticated means, be used to determine the nature of the data being processed by the computer.

D. *Power Surges and Brownouts.*
Computers are susceptible to sudden surges or drops in electrical line voltage. Depending on the importance of the data being processed, efforts should be made to shield the computer from these variations. Electronic devices ranging from inexpensive surge processors to uninterruptible power supplies are available to provide the level of protection required.

III. PHYSICAL SECURITY.

Protection against theft, changes, or unauthorized access to the personal computer or workstation is difficult. Consider the following protective actions:

A. *Location and Construction*
Evaluate potential locations for the computer room. Consider the importance of having direct access from the outside and the need to protect windows. Decide if windows should have bars or electronic detection devices. Should there be a system to control keys and other access devices?

For example, a particular situation might require heavy doors with dead bolts. If the doors are not new, they should have new locks. Seal windows at ground level or protect them with metal bars. Additionally, consider alarms and detection devices.

B. *Computer Room Access.*
Depending on organizational need, restrict access to rooms containing microcomputers to specifically authorized personnel. Consider special precautions for stand alone computers, e.g., those on an employees desk.

C. *Physical Control*
Protect microcomputers with lockable equipment enclosures, lockable power switches, fasteners, and securing devices. Consider devices such as those that sound an alarm when equipment is moved or disconnected from a wall socket.

One example of an advanced device, such as one used by the Department of the Navy, employs a crystal oscillator with various broadcasting frequencies embedded in the microcomputer. Antennas located throughout the area can be used to track any movement of the microcomputer.

Standardized inventory and control forms may be used throughout any organization interested in controlling hardware, software, or data. These forms should contain information about the location of the microcomputer, who is responsible, and any changes made since the original installation. Centrally record the physical location and configuration of each microcomputer.

Some standard devices normally associated with a microcomputer, such as a mouse, internal cards and wires, do not lend themselves well to the above procedures. These devices might be subject to external controls, such as check-out, removal from the machine on a daily basis, etc.

It is particularly important to protect floppy disks from contaminants, unauthorized access, destruction and damage. Procedures should ensure that all diskettes (floppy disks), be labeled before use and stored in a secure place when not in use. One method of protecting diskettes against theft is to hide a signaling device (such as those used in libraries) in the jacket cover of the floppy.

IV. DATA SECURITY

A. *Software Control*

Most popular operating systems used on microcomputers lack adequate security control. Unless measures are taken, this lack of control can lead to serious security violations. The measures may range from use of simple passwords to electronic devices, both of which restrict logon/logoff to authorized persons.

Unless duly authorized, copying computer programs should not be allowed. In addition to the legal problems, program libraries and/or data files become susceptible to sabotage (for example, by the insertion of a computer virus). Further, monitor the use of utility programs to make sure the contents of other programs and stored data have not been changed. Many of these programs can be executed without leaving a trace of their activities.

B. *Backup Procedures.*

Backup procedures are needed to protect against major loss of files or programs and minor problems such as disk read errors. Delineate and enforced a corporate policy to safeguard against potential disasters. Identify the programs and data to be stored, the media on which the files are to be stored, the frequency of backup and who is responsible. The disk backup procedure should be classified as either complete or partial backup. A complete backup treats the disk as a whole and copies it in its entirety to the backup medium (i.e., no attempt is made to identify individual files). A partial backup identifies files to be copied and transfers them to the backup device. Frequently, the partial backup is used to collect those files that have been changed since the last backup.

C. *Recovery Techniques.*

Utilities, such as Norton's Utilities or PCTools, are useful tools to recover files from a disk that has had the File Allocation Table (FAT) damaged or has had files deleted.

D. *Data Encryption and Access Control.*

Various security products have been developed to protect sensitive data stored on microcomputers. These products, sometimes called environment control packages, provide for encryption (encoding) and system/file access control but, also, password protection and audit trail capability. In most cases the program must reside on a hard disk and a system manager must control passwords and system specifications. The program may control the entire system operation from logon to logoff.

A typical product of this type would include these functions:

- Boot Protection – Intruders are not able to bypass the hard disk and boot the system from drive A.
- Password Verification – Each user must enter a password before access to the system is permitted.
- User Segregation – While all users may be able to use any program on the disk, each user's personal files are inaccessible to others.
- Definable User Lockout – Users may be restricted from using programs not essential to their jobs.

- Data Encryption – Data encryption for individual files or for all files may be selected.
- Audit Trail – The audit trail can be customized to include unauthorized access attempts and all system manager functions.

V. SECURITY TRAINING

While most data losses are the result of human error, losses may be minimized by using a continuous program of formal and informal training. Managers must ensure that users develop an attitude that, when something goes wrong, the problem will be reported immediately (i.e., reported problems should be seen as a positive rather than negative gesture). The sooner a security problem has been identified and reported with a complete and correct description, the greater the possibility that the problem can be corrected.

Teaching Considerations

A. SUGGESTED SCHEDULE:

The following sample module plan is based on the offering of three to six hours of lectures.

1. **Ethics..0.2 to.5 hour**
2. **Computer Room Environment................. ....0.2 to.5 hour**
3. **Physical Security.................................. ....0.2 to.5 hour**
4. **Data Security.. .... 0.5 to 1 hour**
5. **Security Training... 0.1to0.2 hour**

B. HOMEWORK AND LAB EXERCISES

Following are examples of Class /Lab/ Paper exercises to enhance the lecture material for the module.

- Visit the microcomputer facility. Interview users and staff, asking their opinions about the ethical considerations discussed in class.
- Examine the computer laboratory, identifying potential problems with physical security.
- Design a security backup procedure for a personal computer/ workstation.
- Recover a ‘lost’ file/program from a disk.

Bibliography

Johnson, Douglas W., *Computer Ethics: A Guide for the New Age*, The Brethren Press, 1984.
This low-cost, readable paperback book introduces critical issues, including: personal data, decision-making and identifying, building and maintaining ethics in a computer society. This book addresses the question of ethics in the indiscriminate use of the personal computer. The concept of what ethics are is proposed and suggestions are made for establishing a code for personal computer use.

Department of Defense, “Personal Computer Security Considerations,” NCSC-WA-002-85, Dec. 1985
This publication provides a general discussion of some issues pertinent to microcomputer security in the home and business environment.

Department of Defense
9800 Savage Road
Ft. Meade, MD 20755-6000
Stop S94

DATAPRO Research Corp., “Data Pro Reports on Information Security”, 1988
This is a collection of reports dealing with all aspect of information security. Reports IS30-xxx-xxx are primarily concerned with the subject of microcomputer security.

DATAPRO Research Corp.
Delran, NJ 08075 (800) 328-2776

Richards, T., Schou, C.D. & Fites, P.E. “Information Systems Security Laws and Legislation,” in *Information Security Modules*, Department of Defense, 1989.

Richards, et. al. review topics, timely laws and legislation about computer security as it relates to the individual and the organization.

SECURITY FUNDAMENTALS

Revised August 1990
Revised May 1995
Revised February 2001

National Information Assurance Training and Education Center
College of Business
Idaho State University

Description:
This module is introductory in nature and provides basic security concepts for undergraduate general business majors and specialized Information Systems Majors. This module outlines and describes the basic requirements for planning, organizing and managing security in an organization. Topics include personal and organizational ethics; hardware and software issues; security and threats to data; recovery, control and audit procedures; and corporate security costs and benefit identification. A bibliography and selected case studies are provided and may be used at the discretion of the instructor to expand any of these topics. This module might be included as part of a Junior level management information systems course or integrated as part of other business courses.

SECURITY FUNDAMENTALS

OBJECTIVES:

The objective of this module is to take the business and information systems major beyond the basic information protection principles and deal with security fundamentals that lay the foundation for specialized advanced study in systems security. Upon successful completion of this module, the student will understand the underlying fundamentals of information security and will be prepared for other course material in the areas of security laws and legislation, communications, advanced systems security and corporate security management.

LEARNING OBJECTIVES

Upon completion of this module, the student should be able to:

- understand the need for security in an organization and identify sensitive resources;
- recognize organizational security mechanisms and basic goals, and recognize the need for communicating policies and procedures within the organization;
- understand ethical issues involved with the use of information systems;
- identify societies and organizations essential to professional development;
- identify procedures associated with establishing a personnel security program;
- identify procedures associated with establishing a physical security program;
- recognize significant security areas other than those covered explicitly in this module;
- define threat, vulnerability and control in an organization;
- recognize procedures necessary for data security and recovery;
- identify the components of an audit trail; and
- identify the costs and benefits associated with secure systems.

PREREQUISITE:

Completion of the first two modules, “Introduction to Information Protection” and “PC/Workstation Security” would be useful. Some basic knowledge about computer information systems and basic business courses is desirable. The student should have some computer laboratory experience.

Topic Outline

I. Planning
A. Security As Part Of The Total Organization
B. Understanding The Organization
C. Identifying Sensitive Data
D. Controlled Sharing Of Information And Resources
E. Specific Needs:
  1. Secrecy
  2. Integrity
  3. Availability
F. Analysis & Design
II. Organizational Policies & Procedures
A. Scope Of Security Mechanisms
  1. Administrative
  2. Procedural
  3. Physical
  4. Operational
  5. Technical
B. Basic Goals
  1. Prevention
  2. Deterrence
  3. Containment
  4. Detection
  5. Recovery
C. Written Management Policies & Procedures
  1. Documentation
  2. Manuals
III. Ethics And Professionalism
A. Ethics
  1. Responsible Decision-Making
  2. Confidentiality & Privacy
  3. Piracy
  4. Fraud & Misuse
  5. Liability
  6. Copyright
  7. Trade Secrets
  8. Sabotage
B. Laws And Legislation
C. Professionalism
  1. National Computer Security Center
     National Computer Security Conference
  2. National Bureau Of Standards
  3. The Computer Security Institute
  4. Computer Professionals For
     Social Responsibility and CPSR Newsletter
  5. Data Processing Management Association
  6. Security Management Magazine
  7. Licensing And Certification
IV. Personnel Security
A. Personnel Policies
  1. Hiring Practices
  2. Training
  3. Access Rights And Privileges
  4. Rules For Granting And Revoking Privileges
  5. Separation Of Privileges And Roles
  6. Adverse Actions
  7. Termination Practices
V. Physical Security
A. Location
  1. Access Versus Security
  2. Rooms, Doors, Windows, Keys
B. Environment
  1. Radio Frequency Interference [RFI]
  2. Cooling
  3. Cabling
  4. Power
VI. System Security
A. PC & Workstations
B. Database
C. Networks And Communications
D. Operating Systems
E. Application Software
F. Systems Security
G. Systems Architecture
H. Audit And Control
I. Corporate Security Management
VII Threats And Vulnerability
A. Natural Disasters
  1. Fire
  2. Flood
  3. Brown-Outs
  4. Lightning
B. Accidental
  1. Disclosure Of Data
  2. Modification / Destruction Of Data
  3. Faulty Software
  4. Residual Data
  5. Wrong Parameters
C. Malicious
  1. Trap Doors
  2. Trojan Horse
  3. Tampering
  4. Snooping Or Browsing
  5. Intentional Disclosure Of Data
  6. Viruses
D. Locus Of Attack
  1. Terminals
  2. Hosts
  3. Front-Ends
  4. Gateways
  5. Links
  6. Packet-Switches
  7. PC / Workstations
VIII. Data Security And Recovery
A. Floppy Diskettes
B. Hard Disks
C. Back-Up
D. Recovery Principles
E. Utilities

F. Security Training
  1. User Training
  2. User Help
G. Encryption
IX. Control And Audit
A. Logon Authentication
B. Access Control
C. Audit
  1. Event Classes
  2. Audit Selectivity
  3. Management Of Audit Trails
D. Relationship Between Operations, Management & Audit
X. Costs And Benefits
A. Accessibility Versus Secrecy
B. Costs
  1. Money & Time For Development, Installation, Procurement, & Maintenance Of Security Measures
  2. Special Skills
  3. Performance
  4. Productivity
  5. Training Time
  6. Compatibility - Of Equipment, Procedures...
C. Benefits
  1. Precise Definition Of Requirements
  2. Value Of Information
  3. Peace Of Mind
  4. Productivity
  5. Protection From Legal Liability
  6. Protection From Loss Of Assets/Company
  7. Good-Will
  8. Privacy
    a. Individual
    b. Corporate
    b. Governmental

Annotated Outline

I. PLANNING

A. Security As Part Of The Total Organization

Information security is not simply software or hardware security; it does not stand apart from the total organization. An organization's policies, plans and procedures may affect security needs and security practices may affect those polices, plans or procedures. The important point is that a secure system is integral part to total organization.

B. Understanding The Organization

If a secure system is to be part of the total organization, then one must first understand the organization, its goals and objectives, policies and procedures. If an organization's objectives are unclear, implementing new technology will not help. If an organization's procedures are not secure, new technology will not make it any more secure. Understanding the organization is the first step in planning for a secure system.

C. Identifying Sensitive Data

After establishing a clear understanding of the organization's function and how it is to accomplish its objectives, the first step in a secure system is to identify sensitive data. Recognize specific levels of security and that each may not be equally valuable (e.g., no need to spend $1,000 to protect a hammer). Identifying sensitive data and determining their value before the fact is a most difficult task for any organization. Unfortunately for most MIS directors, management will more easily recognize the true value of data after the data are compromised.

D. Controlled Sharing of Information and Resources

Sharing information and resources is increasingly possible through networking, communications and connectivity. As this sharing increases, the problems of information security increase exponentially. The problem for management is one of both encouraging increased productivity using technology while maintaining what will probably be an increasingly insecure system.

E. Specific Needs

Security addresses three principal needs: secrecy, integrity, and availability. Secrecy involves preventing the unauthorized disclosure of information and unauthorized use of information and resources. Integrity involves preventing the unauthorized creation, modification or deletion of information and ensuring the consistency of information. Availability involves preventing the unauthorized delay or denying the use of information and resources.

F. Analysis and Design

Formalizing a secure system begins with appropriate organizational analysis and identification of sensitive data and procedures for handling those data. An appropriate place to introduce this material in more detail is in an information systems analysis and design course.

II. ORGANIZATIONAL POLICIES & PROCEDURES

It is critical that policies procedures be loped which reflect the significance of the information resource

A. *Scope Of Security Mechanisms*
Security policies specify the rules that govern how information is to be protected; security mechanisms enforce these policies. Since a secure system is one that should be part of the total organization, the scope of the security mechanism may include all the administrative, procedural, physical, operational and technical aspects of the organization.

B. *Basic Goals*
Basic goals of a secure system are:

- Prevention includes those organizational, operational and physical methods thought necessary to keep a system secure from both internal and external penetration;
- Deterrence includes those policies, procedures and actions designed to discourage penetration of the system;
- Containment focuses on keeping sensitive data within the system;
- Detection means to find the nature, existence, presence or fact of the system penetration;
- Recovery is the action necessary to restore a system's computational capability and data files after a system failure or penetration. A disaster plan is part of recovery.

C. *Written Management Policies & Procedures*
Once sensitive data are identified, and policies and procedures for handling sensitive data have been established, these policies and procedures must be communicated to those who are affected. A variety of methods including training and a security manual may be used for communicating this information.

III. ETHICS AND PROFESSIONALISM

There are several ways of identifying and deciding ethical issues. One of the most common ways of categorizing these approaches is the rules vs. consequences criteria. The first argues that our actions should be guided by general rules or principles: do not harm; tell the truth; do not steal; respect for persons. The second argues that we should assess the "rightness" of an action or decision by the consequences that will likely result. Most commonly the second approach identifies some "value" or values, and measures the actions by the extent to which these values are or are not enhanced, or progress made toward certain goals, such as a better life for all.

On reflection is should be clear that there is no consensus about which of these is the more appropriate.

The foundation of all security systems is formed by moral principles and practices of those people involved and the standards of the profession. That is, while people are part of the solution, they are also most the problem. Security problems with which an organization may have to deal include: responsible decision making, confidentiality, privacy, piracy, fraud & misuse, liability, copyright, trade secrets, and sabotage. It is easy to sensationalize these topics with real horror stories; it is more difficult to deal with the underlying ethical issues involved.

A. *Ethics*

1. **Ethics and Responsible Decision-Making**
The foundation of all security systems is formed by moral principles and practices of those people involved and the standards of the profession. That is, while people are part

of the solution, they are also most the problem. Security problems with which an organization may have to deal include: responsible decision making, confidentiality, privacy, piracy, fraud & misuse, liability, copyright, trade secrets, and sabotage. It is easy to sensationalize these topics with real horror stories; it is more difficult to deal with the underlying ethical issues involved.

The student should be made aware of his individual responsibility in making ethical decisions associated with information security.

2. Confidentiality & Privacy

Computers can be used symbolically to intimidate, deceive or defraud victims. Attorneys, government agencies and businesses increasingly use mounds of computer generated data quite legally to confound their audiences. Criminals also find useful phony invoices, bills and checks generated by the computer. The computer lends an ideal cloak for carrying out criminal acts by imparting a clean quality to the crime.

The computer has made the invasion of our privacy a great deal easier and potentially more dangerous than before the advent of the computer. A wide range of data are collected and stored in computerized files related to individuals. These files hold banking information, credit information, organizational fund raising, opinion polls, shop at home services, driver license data, arrest records and medical records. The potential threats to privacy include the improper commercial use of computerized data, breaches of confidentiality by releasing confidential data to third parties, and the release of records to governmental agencies for investigative purposes.

The basic law that protects our privacy is the Fourth Amendment to the United States Constitution, which mandates that people have a right to be secure in homes and against unreasonable search and seizure. In addition, many laws have been enacted to protect the individual from having damaging information stored in computerized databases.

3. Piracy

Microcomputer software presents a particular problem since many individuals are involved in the use of this software. Section 117 of the copyright laws, specifically the 1980 amendment, deals with a law that addresses the problem of backup copies of software. This section states that users have the right to create backup copies of their software. That is, users may legally create a backup copy of software if it is to be held in archive. Many software companies provide a free backup copy to users that precludes the need for to users purchase software intended to defeat copy protection systems and subsequently create copies of their software. If the software purchased is actually leased, you may in fact not even be able to make backup copies of the software. The distinction between leasing and buying is contained within the software documentation. The copyright statement is also contained in the software documentation. The copyright laws regarding leased material state that the leasor may say what the leaseholder can and cannot do with the software. So it is entirely up to the owner of the software as to whether or not users may make backup copies of the software. At a time when federal laws relating to copyright protection are evolving, several states are considering legislation that would bar unauthorized duplication of software.

The software industry is prepared to do battle against software piracy. The courts are dealing with an increasing number of lawsuits concerning the protection of software.

Large software publishers have established the Software Protection Fund to raise between $500,000 and $1 million to promote anti-piracy sentiment and to develop additional protection devices.

4. Fraud & Misuse

The computer can create a unique environment in which unauthorized activities can occur. Crimes in this category have many traditional names including theft, fraud, embezzlement, extortion, etc. Computer related fraud includes the introduction of fraudulent records into a computer system, theft of money by electronic means, theft of financial instruments, theft of services, and theft of valuable data.

5. Liability

Under the UCC, an express warranty is an affirmation or promise of product quality to the buyer and becomes a part of the basis of the bargain. Promises and affirmations made by the software developer to the user about the nature and quality of the program can also be classified as an express warranty. Programmers or retailers possess the right to define express warranties. Thus, they have to be realistic when they state any claims and predictions about the capabilities, quality and nature of their software or hardware. They should consider the legal aspects of their affirmative promises, their product demonstrations, and their product description. Every word they say may be as legally effective as though stated in writing. Thus, to protect against liability, all agreements should be in writing. A disclaimer of express warranties can free a supplier from being held responsible for any informal, hypothetical statements or predictions made during the negotiation stages.

Implied warranties are also defined by the UCC. These are warranties that are provided automatically in every sale. These warranties need not be in writing nor do they need to be verbally stated. They insure that good title will pass to the buyer, that the product is fit for the purpose sold, and that it is fit for the ordinary purposes for which similar goods are used (merchantability)..

6. Patents and Copyright Law

A patent can protect the unique and secret aspect of an idea. It is very difficult to obtain a patent compared to a copyright (please see discussion below). With computer software, complete disclosure is required; the patent holder must disclose the complete details of a program to allow a skilled programmer to build the program. Moreover, a United States software patent will be unenforceable in most other countries.

Copyright law provides a very significant legal tool for use in protecting computer software, both before a security breach and certainly after a security breach. This type of breach could deal with misappropriation of data, computer programs, documentation, or similar material. For this reason the information security specialist will want to be familiar with basic concepts of to copyright law.

The United States, United Kingdom, Australia, and many other countries have now amended or revised their copyright legislation to provide explicit copyright laws to protect computer program. Copyright law in the United States is governed by the Copyright Act of 1976 that preempted the field from the states. Formerly, the United States had a dual state and Federal system. In other countries, such as Canada, the courts have held that the un-revised Copyright Act is broad enough to protect computer programs. In many of these countries the reform of copyright law is actively underway.

7. **Trade Secrets**
   A trade secret protects something of value and usefulness. This law protects the unique and secret aspects of ideas, known only to the discoverer or his confidants. Once disclosed the trade secret is lost as such and can only be protected under one of the following laws. The application of trade secret law is very important in the computer field, where even a slight head start in the development of software or hardware can provide a significant competitive advantage.

8. **Sabotage**
   The computer can be the object of attack in computer crimes such as the unauthorized use of computer facilities, alternation or destruction of information, data file sabotage and vandalism against a computer system. Computers have been shot, stabbed, short-circuited and bombed.

B. Laws and Legislation

The types and numbers of security laws and legislation at all governmental levels are expanding rapidly. Often, we forget that such legislation may affect each of us, as well as the organization. For more information see module four: "Information Systems Security Laws and Legislation".

The following items should be discussed in terms of both Ethics and Law. Where do Ethics and Law converge? Are they the same? The foundations of all secure systems are the moral principles and practices and the professional standards of all employees of the organization, i.e., while people are part of the solution, they are also most of the problem. The following issues are examples of security problems which an organization may have to deal with:

C. Professionalism

Students should be encouraged to become involved professionally while they are in school and to continue their professional involvement throughout their career. Several societies and professional organizations are concerned with security, including:

- The Computer Security Institute
- Computer Professionals for Social Responsibility
- Data Processing Management Association
- Security Management Magazine
- Licensing and Certification

a. Institute For Certification of Computer Professionals

b. IISSCC (ISC^2)

In addition, there are two government agencies actively involved in the professionalism. The first is the National Computer Security Center that hosts the National Computer Security Conference each year. The second is NIST that has an outreach charter. Discuss Costs and benefits of professional participation.

IV. PERSONNEL SECURITY

Most security problems, whether accidental or malicious, begin with people; of these people, by far, most of them come from within the organization. The foundation for dealing with people problems is to try to eliminate the potential for problems before they happen. Accomplish this by anticipating where personnel might cross paths with secure data and by contemplating the consequences. Formalize the results of this analysis in the personnel section of the security policy and procedures manual and communicate the results to those people involved. Each of the items listed below, from hiring to termination, becomes a significant part of a secure system.

A. *Hiring Practices*
Always perform background investigations of employees before hiring them. One should perform some form a background investigation.

B. *Training*

C. *Access Rights And Privileges*

D. *Rules For Granting And Revoking Privileges*

E. *Separation of Privileges and Roles*

F. *Adverse Actions*

G. *Termination Practices*

This segment of the module might be expanded upon in a personnel management course.

V. PHYSICAL SECURITY

Ideally planning for physical security begins with an evaluation of potential locations for the computing system and of sensitive data flow both internally and externally. One may get a great buy on a building with large glass windows on Main Street in Beirut, but from a security standpoint is it a good deal? As with all security issues, identify the level of data security needed and the cost/benefits before arriving at the appropriate decision. In class discussions consider the following.

A. *Location*
The location of the information processing function has an impact on security system design.

1. Access versus security

Access control is another important countermeasure to provide network security. This is achieved by identifying the privileges of a user to access information or use the services provided by elements of the network and to administer the operation of the process to insure that the user can only access and use what he or she has been granted permission.

Various security products have been developed to protect sensitive data stored on microcomputers. These products, sometimes called environment control packages, provide for encryption (encoding) and system/file access control but, also, password protection and audit trail capability. In most cases the program must reside on a hard disk and a system manager must control passwords and system specifications. The program may actually control the entire system operation from logon to logoff.

A typical product of this type would include these functions:

- Boot Protection – Intruders are not able to bypass the hard disk and boot the system from drive A.
- Password Verification – Each user must enter a password before access to the system is permitted.
- User Segregation – While all users may be able to use any program on the disk, each user's personal files are inaccessible to others.

- Definable User Lockout – Users may be restricted from using programs not essential to their jobs.
- Data Encryption – Data encryption for individual files or for all files may be selected.
- Audit Trail – The audit trail can be customized to include unauthorized access attempts and all system manager functions.

2. Rooms, Doors, Windows, Keys

a. *Location and Construction*

Evaluate potential locations for the computer room. Consider the importance of having direct access from the outside and the need to protect windows. Decide if windows should have bars or electronic detection devices. Should there be a system to control keys and other access devices?

For example, a particular situation might require heavy doors with dead bolts. If the doors are not new, they should have new locks. Seal windows at ground level or protect them with metal bars. Additionally, consider alarms and detection devices.

b. *Computer Room Access.*

Depending on organizational need, restrict access to rooms containing microcomputers to specifically authorized personnel. Consider special precautions for stand alone computers, e.g., those on an employees desk. Resource sharing systems, remote terminals should be available only to selected individuals. This access may be controlled by one or more of the following:

- Locked doors.;
- Posted guards;
- Other approved restraints.

c. *Physical Control*

Protect microcomputers with lockable equipment enclosures, lockable power switches, fasteners, and securing devices. Consider devices such as those that sound an alarm when equipment is moved or disconnected from a wall socket.

One example of an advanced device, such as one used by the Department of the Navy, employs a crystal oscillator with various broadcasting frequencies embedded in the microcomputer. Antennas located throughout the area can be used to track any movement of the microcomputer.

Standardized inventory and control forms may be used throughout any organization interested in controlling hardware, software, or data. These forms should contain information about the location of the microcomputer, who is responsible, and any changes made since the original installation. Centrally record the physical location and configuration of each microcomputer.

Some standard devices normally associated with a microcomputer, such as a mouse, internal cards and wires, do not lend themselves well to the above procedures. These devices might be subject to external controls, such as check-out, removal from the machine on a daily basis, etc.

It is particularly important to protect floppy disks from contaminants, unauthorized access, destruction and damage. Procedures should ensure that all diskettes (floppy disks), be labeled before use and stored in a secure place when not in use. One method of protecting diskettes against theft is to hide a signaling device (such as those used in libraries) in the jacket cover of the floppy.

- One should locate the media library in an area secure from explosion or other dangers.
- Recall that security includes backup file systems at a secondary location for both the programs and the associated documentation. Essential programs, software systems, and associated documentation of programs in the library are located in a locked vault or a secured area.

B. Environment

Control of the environment a fundamental issue in information security.

1. Radio Frequency Interference (RFI)

All electronic equipment produce radiation and emanations of varying frequencies. Take care that the computer will operate in the environment that contains emanations from other electronic devices and that the computer will not interfere with other electronic devices.

If care is not taken, RFI may be received outside the computer facility and, by sophisticated means, be used to determine the nature of the data being processed by the computer.

2. Cooling

While a personal computer is somewhat insensitive to its environment, some attention to the environment will prolong the life and increase the safety of data stored in the machine. A rule of thumb to apply when considering the physical environment is, "If you are comfortable, the computer is comfortable."

3. Cabling

Cables should be routed to minimize both RFI and unauthorized personnel. Cables and Cableways should be protected from both fire and water damage.

4. Power Surges and Brownouts.

Computers are susceptible to sudden surges or drops in electrical line voltage. Depending on the importance of the data being processed, efforts should be made to shield the computer from these variations. Electronic devices ranging from inexpensive surge processors to uninterruptible power supplies are available to provide the level of protection required.

VI. SYSTEM SECURITY

Other significant sections of an information system must be considered when developing and maintaining a secure system. Most items listed below are dealt with in separate security modules. The appropriate place to deal with these detailed aspects of a secure system is in a separate course for each of these topics.

When using this basic module, remind students about the importance of security in each of the major areas listed below.

A. *PC & Workstations*

B. *Database*

C. *Networks and Communications*

D. *Operating Systems*

E. *Application Software*

F. *Systems Security*

G. *Systems Architecture*

H. *Audit and Control*

I. *Corporate Security Management*

Ultimately these areas must be considered together as a system.

VII. THREATS AND VULNERABILITY

A. *Natural Disasters*

Disasters can take all shapes and forms; natural disasters, like those listed, are common security problems because one has no control over the original cause of the problem. Preparing for disaster is a vital part of a disaster recovery or contingency plan. Examples of Natural Disasters that should be discussed are:

1. **Fire**

   The threat of fire should not be under estimated. One should provide specific site documentation for fire risk and exposure. This documentation should contain at a minimum:

   a. The construction techniques that demonstrate the fire resistance of the building containing the system. Raised floors and ceilings, curtains, rugs, furniture, and drapes should be from non combustible materials.
   b. The procedures used to manage the paper and other combustible supplies for the computer facilities. In addition, this should document the control of inflammable or dangerous activities in areas surrounding the computer room.
   c. The storage of magnetic media outside the computer room.
   d. The periodic training of operators in fire fighting techniques and assigned responsibilities in case of fire.
   e. The use of water for fire protection is usually advised. The two major forms of protection are.
      1) Automated carbon dioxide. If so, do all personnel have training in the use of gas masks and other safety devices.
      2) Halogenated agents
2. **Flood**

   The potential for flood should be minimized by locating computer equipment above the flood plane. Another source of flood damage is the water distribution and fire protection systems. Water should not flow through pipes above the computer facility.

3. **Brown-outs**

   Computers are susceptible to sudden surges or drops in electrical line voltage. Depending on the importance of the data being processed, efforts should be made to shield the computer from these variations. Electronic devices ranging from inexpensive surge processors to uninterruptible power supplies are available to provide the level of protection required.

4. **Lightning**
   Adequate isolation and grounding should be provided for both the computer equipment and for the power supply.

B. *Accidental Acts (Threats)*
Many threats to a system result from unintentional errors created either by a user or by the system itself. The most common forms of accidental threats are caused by employee mistakes, frequently resulting from poor training and improper use of tools. Possible results include unintentional damage to the system, modification or destruction of user programs or data, disclosure of sensitive information, or residual data that the user or management cannot find. On-going training programs, both formal and informal, can help prevent many of these problems. At a minimum the following should be discussed:

1. **Disclosure of data**

2. **Modification/Destruction of data**

3. **Faulty software**

4. **Residual data**

5. **Wrong parameters**

C. *Malicious Acts (Threats)*
These threats are the result of deliberate attempts to circumvent or defeat the systems' protection mechanisms or to exploit the weaknesses in such mechanisms. Many entertaining anecdotes illustrate the items listed. All too often, however, it is easy to overlook the ethical, legal and potentially damaging implications of such activities. The following malicious acts should be supplemented from the current news when appropriate:

1. **Trap doors**
   A trap door is an embedded segment of code which allow one to circumvent the normal security or administrative protection of a system.

2. **Trojan Horse**
   The Trojan horse technique of penetration "consists of supplying the computer with what is perceived appropriate and acceptable information, but in reality contains secret instructions for unauthorized behavior."

3. **Tampering**
   Systems should be designed such that the data are protected from unauthorized changes or modification.

4. **Snooping or browsing**
   One should design systems such that user access is contained to data and information for which they have a need.

5. **Intentional disclosure of data**

6. **Viruses**
   Computer viruses are particularly new and dangerous form of active intrusion. These computer programs infiltrate a computer system and attack the operating system, application programs, and data in the same way a cancer virus or retro viruses attack the human system. They can lie dormant for a time, hidden from the user or operator of the system, before they become active. By the time they are discovered, a great deal of damage may have occurred and much data may have been destroyed and lost. Viruses are composed of three parts:

   a. A mission component (such as to delete files, send data to a certain user, etc.);
   b. A trigger mechanism (which activates at a specific time or with the occurrence specific event, e.g., the person's name not being on the payroll list); and
   c. A self-propagating component (whereby it attaches itself to files, programs, or whatever the creator of the virus is in search of).

   The threat from viruses increases when interconnected systems are involved because the virus can be injected into one element and quickly spread to other interconnected elements or have access to the infected element.

D. Locus of Attack

The locus of attack is a place or places from which an attack upon a system may originate. The locus of attack becomes increasing complex as a system grows through networking, communications and connectivity. Additional material should be introduced in a networking and communications course. Each item listed provides an example of potential vulnerability of sensitive data.

1. **Terminals**
   Terminals are frequently in less well controlled facilities. Plans should be made for passwords and physical interlocks to minimize the terminal as a source of information compromise.

2. **Hosts**

3. **Front-ends**

4. **Gateways**
   The gateway from another system should be protected carefully. One should not rely on the security of the distal end of the link.

5. **Links**

6. **Packet-switches**

7. **PC/workstations**
   PC/workstations are frequently in less well controlled facilities. A workstation may harbor software that at some time in the future may attack your security system. Plans should be made for passwords and physical interlocks to minimize the workstation as a source of information compromise.

VIII. DATA SECURITY AND RECOVERY

Students need to know that data security and recovery procedures exist, but most of all that a useful procedure for every user is the practice of making backup copies of all significant data. Security systems for those backup copies are often forgotten. Basic handling and care of floppy diskettes is a beginning point for the novice user.

Understanding data storage and recovery techniques using commercial software utilities is fundamental for regular users of personal computers. Prevent lost data by training users to use equipment properly and to identify the exact sequence of events that happened before something went wrong. One should emphasize the importance of a bound log book. This is often a great aid to those who must “undo” the problem. For more sensitive data, consider encryption techniques.

IX. CONTROL AND AUDIT

The audit trail is a permanent record of every transaction that has taken place in a system. Who, when, where, and what are requirements for an audit trail and are necessary for a secure system. Control of the audit trail determines the success of the system. Audit trails may be required by law or company regulation, and may be used for backup and recovery or an analysis of errors. In data security they can be used for detecting security violation and as a means for security-violation deterrence. Discuss the relationship between operations, management and the audit function.

X. COSTS AND BENEFITS

The issue of data security can be reduced to the desire for data accessibility by an individual versus the need for data secrecy by an organization. Analysis of organizational data needs compared with its sensitive data analysis report is one starting point for doing a cost-benefit analysis. One method for doing this is a risk matrix model. Information assets can be compared with data threats and vulnerability. The value of the data is its worth in case of loss. The obvious difficulties of interpretation do not preclude the use of this method to help in the decision-making process. The following are important issues for discussion.

A. *Accessibility Versus Secrecy*
   If information is to be used, it must be accessible or users will not avail themselves of it. If it is too available, it may be distributed to unauthorized individuals.

B. *Costs*
   1. **Money and time for development, installation, procurement, and maintenance of security measures**

   2. **Special skills**

3. **Performance**

4. **Productivity**

5. **Training time**

6. **Compatibility - of equipment, procedures,...**

C. Benefits

1. **Precise definition of requirements**

2. **Value of information**

3. **Peace of mind**

4. **Productivity**

5. **Protection from legal liability**

6. **Protection from loss of control of assets / company**

7. **Good-will**

8. **Privacy**
   - *a. Individual*
   - *b. Corporate*
   - *c. Governmental*

Teaching Considerations

A. SUGGESTED SCHEDULE:

The following sample module plan is based on the offering of six to nine hours of lectures with outside lab and homework time. To cover adequately each area in this module, integrate the material into other business and information systems courses.

1. **Planning..0.5 hour**
2. **Organizational Policies and Procedures...1.0 hour**
3. **Ethics and Professionalism...0.5 hour**
4. **Personnel Security...0.5 hour**
5. **Physical Security..0.5 hour**
6. **System Security...0.5 to 1 hour**
7. **Threats and Vulnerability..0.5 to 1 hour**
8. **Data Security and Recovery...0.5 to 1 hour**
9. **Control and Audit...0.5 hour**
10. **Costs and Benefits...0.5 to 1 hour**

B. HOMEWORK AND LAB EXERCISES:

Following are examples of exercises to enhance the lecture material for this module:

1. Class/Paper exercises:
   a. Brainstorm and graph the flow of data in an organization then identify sensitive resources;
   b. List organizational security mechanisms that might be used to control the sensitive resources in (a).
   c. Take the position of the "bad guy" and justify the ethical standpoint of "why you went wrong."
   d. Identify corporate policies and procedures for dealing with sensitive resources, and show how these policies and procedures might be communicated to the appropriate personnel.
2. Lab exercise - Visit the microcomputer lab and identify:
   a. What is GOOD about security. Why?
   b. What is POOR about security. Why?

Bibliography

Schou, C.D., Fites, P.E., & Burgess, J.D., "Corporate Security Management," in *Information Security Modules*, Department of Defense, 1989.
Consider this the capstone security module in this document. Emphasis is on the management of a corporate level data security program.

Fites, Philip E., Martin P. J. Kratz, and Alan F. Brebner, *Control and Security of Computer Information Systems*, W. H. Freeman/Computer Science Press, September. 1988.

A textbook intended to support college level courses in computer security for technicians and accountants, or to serve as a reference for computer law courses. Contains considerable detail on the material mentioned in this module. A useful reference as well.

Computer Security Institute, Computer Security Handbook: Computer Security Institute, updated yearly.
This publication is a compilation of timely sensitivity related articles and monographs. Chapter headings include Managing Security, Protecting the Data Center Communication Security, Disaster Recovery Planning, and Auditing. A good general reference of timely information.

The Computer Security Institute publishes The Computer Security Journal and a computer security handbook. Computer Security Institute, 360 Church Street, North Borough, MA. 01532, (508) 393-2600.

Johnson, Douglas W., *Computer Ethics: A Guide for the New Age*, The Brethren Press, 1984.
This low-cost, readable paperback book introduces critical issues, including: personal data, decision-making and identifying, building and maintaining ethics in a computer society. This book addresses the question of ethics in the indiscriminate use of the personal computer. The concept of what ethics are is proposed and suggestions are made for establishing a code for personal computer use.

Computer Professionals for Social Responsibility, Inc., P.O. Box 717, Palo Alto, CA 94301, 415/322-3778.
CPSR is an organization for computer professionals concerned about social issues. There are active chapters around the world. They produce a newsletter.

Mandell, Steven L., *Computer Data Processing, and the Law,* West Publishing Company, Minnesota, 1984.
This book has been designed especially for the functional aspects of data processing management.

Davis, G. G., *Software Protection, Practical and Legal Steps to Protect and Market Computer Programs*, Van Nostrand Reinhold, New York, 1985.
An academic discussion of intellectual property rights, copyright, unresolved problems with copyright, software warranties, export controls, and infringement remedies.

Richards, T., Schou, C.D. & Fites, P.E. “Information Systems Security Laws and Legislation,” in *Information Security Modules*, Department of Defense, 1989.
Richards, et. al. review topics, timely laws and legislation about computer security as it relates to the individual and the organization.

Institute For Certification of Computer Professionals, 2200 E. Devon Avenue, Suite 268, Des Plaines, IL 60018. 312/299-4227
This organization administers professional certificate programs and is sponsored by thirteen other professional organizations.

DATAPRO Research Corp., *Data Pro Reports on Information Security*, 1988
This is a collection of reports dealing with all aspect of information security. Reports IS30-xxx-xxx are primarily concerned with the subject of microcomputer security.

DATAPRO Research Corp.

Delran, NJ 08075 (800) 328-2776

Spiro, Bruce E. & Schou, Corey D., "System Security," in *Information Security Modules*, Department of Defense, 1988.

A detailed review of security issues and the integration of these details into an organizational security program.

Walston, Claude, and Lisa Hinman, *Communications Security* IDA Memorandum security breach dealing with possible misappropriation of data, computer programs blueprints, plans, laboratory notes or similar material.

Whiteside, T., *Computer Capers*, Mentor, 1978.

Many vignettes of some early "tales of electronic thievery, embezzlement, and fraud" that brought the problem of data security to our attention. These stories can be used with reports of current problems, for example from The Wall Street Journal or Fortune magazine.

Voydock, V. and Kent, S., "Security Mechanisms in High-Level Network Protocols," *ACM Computing Surveys*, Vol. 15, No. 2, June 1983, pp. 135-171.

Threats, cryptographic controls, and use of end-to-end encryption in networks.

Denning, D.E., *Cryptography and Data Security*, Addison-Wesley, 1983.

Presently this is one of the principal textbooks in computer security. Good as a background reference.

Burgess, J.D. & Watts, R.T., "PC/Workstation Security," in *Information Security Modules*, Department of Defense, 1989.

This module gives an introduction to security problems that one may have when working with a stand-alone PC or workstation (networked PCs or workstations are NOT considered here). This material is useful, for a one-person business as well as individual user who is part of a larger organization.

National Computer Security Center, "A Guide to Understanding AUDIT in Trusted Systems", NCSC-TG-001-87, 1987. Department of Defense, 9800 Savage Road, Fort George G. Meade, MD 20755-6000

The guidelines described in this document provide a set of good practices related to the use of auditing in automatic data processing systems used for processing classified and other sensitive information.

INFORMATION SYSTEMS SECURITY:
LAWS AND LEGISLATION

Revised August 1990
Revised May 1995
Revised February 2001

Corey D. Schou, Ph.D.
National Information Assurance Training and Education Center
College of Business
Idaho State University
Philip E. Fites, MBA, CSP, CDP
Data Processing Management Association

Description
This module may be used in both Information Systems courses, as well as courses in the common body of knowledge, as defined by the American Assembly of Colleges and Schools of Business (AACSB). This module is intended to be part of a junior or senior level course in a Management Information Systems curriculum that covers the management aspects of information systems. For example, it might be included as a module in the DPMA Model Curriculum for Undergraduate Computer Information Systems courses CIS/86-18 (Information Resource Planning and Management) or CIS/86-14 (Computer Control and Audit). It could also be included as part of MIS or Legal Environment courses.

INFORMATION SYSTEMS SECURITY: LAWS AND LEGISLATION

OBJECTIVES:

This module addresses some of the legal specifics that relate to information security and liability. Because computer laws are changing rapidly, the professional working in information security, who makes contact with the law is strongly advised to obtain knowledgeable legal advice.

The purpose of this module is to provide a basic framework for understanding the role of law in planning, implementing and sustaining information security systems. The information specialist must understand a number of basic concepts related to diverse areas of law in order to more fully appreciate the design, implementation and execution of a truly comprehensive information security program. This module does not purport to provide specific legal advice about any particular situation.

Obviously one module cannot hope to address all areas of law that might be relevant to the information security manager. Local variations of general principles and application of law relating to possession and control of real property, the torts of false arrests, malicious prosecution, the tort libel, slander, conspiracy to injure, interference with advantageous business relationships, conversion, and such other general areas cannot be adequately dealt with in this module. The reader should review current introductory texts, periodicals, court cases and legislation in appropriate areas of law. Selected references appear at the end of this module.

LEARNING OBJECTIVES

Upon completion of this module, the student should be able to:

- understand the interrelationship between various areas of law and security system design;
- provide a general analysis of security situations involving aspects of copyright law;
- provide a general analysis of security situations involving aspects of terms of license agreements;
- provide a general analysis of security situations involving aspects of obligations of confidence or other aspects of trade secrets law;
- conduct a basic analysis, review and assessment of terms of non-disclosure agreements;
- analyze and review computer crime legislation applicable in a particular jurisdiction against the backdrop of computer and information crime legislation in other jurisdictions.

PREREQUISITE:

A basic understanding of computer concepts, business concepts and business law is required.

Topic Outline

I. The Underlying Problem
   A. Theft of Hardware and data, Copying Software
   B. Fraud
   C. Physical Abuse
   D. Misuse of Information
   E. Issues of Adjudication and Regulation
II. Laws as Tools for Information Security
   A. Privacy Laws and Legislation
   B. Intellectual Property Laws
      Trade Secrets Law
      Patent Law
      Copyright Law
      Trademark Law
   C. Federal Laws
   D. State Statutes
   E. DPMA Model Computer Crime Bill
III. Laws and Legislation as Legal Options to Control Computer Crime
   A. License Agreements
   B. Intellectual Property Rights
   C. Employee Non-Disclosure Considerations
   D. Contracts
   E. Warranties for Software and Hardware

Annotated Outline

I. UNDERLYING PROBLEMS

A. *Theft of Hardware and Data*

When computers were first introduced some thirty years ago, business and government were quick to make use of their enormous potential as an information processing machine. About the same time, a number of enterprising individuals also saw the potential of these machines for personal gain and began to match their wits against them and find ways to use the computer for criminal purposes. The average armed robbery nets about $9,000 and the average computer fraud totals about $450,000. This is a high yield, low risk crime.

One area of computer crime is the theft of hardware and software. The outright theft of hardware and software is often reported and identified as the prime motive for a crime. For example, in one recent case over $300,000 worth of computer equipment was stolen using phony invoices. In some instances only parts of the computer are targeted. A number of DEC computer installations were recently hit by a rash of break-ins that result in the theft of VAX printed circuit boards. One haul consisted of 22 boards worth about $450,000.

B. *Fraud*

The computer can create a unique environment in which unauthorized activities can occur. Crimes in this category have many traditional names including theft, fraud, embezzlement, extortion, etc. Computer related fraud includes the introduction of fraudulent records into a computer system, theft of money by electronic means, theft of financial instruments, theft of services, and theft of valuable data.

C. *Physical Abuse*

The computer can be the object of attack in computer crimes such as the unauthorized use of computer facilities, alternation or destruction of information, data file sabotage and vandalism against a computer system. Computers have been shot, stabbed, short-circuited and bombed.

D. *Misuse of Information and Privacy Issues*

Computers can be used symbolically to intimidate, deceive or defraud victims. Attorneys, government agencies and businesses increasingly use mounds of computer generated data quite legally to confound their audiences. Criminals also find useful phony invoices, bills and checks generated by the computer. The computer lends an ideal cloak for carrying out criminal acts by imparting a clean quality to the crime.

The computer has made the invasion of our privacy a great deal easier and potentially more dangerous than before the advent of the computer. A wide range of data are collected and stored in computerized files related to individuals. These files hold banking information, credit information, organizational fund raising, opinion polls, shop at home services, driver license data, arrest records and medical records. The potential threats to privacy include the improper commercial use of computerized data, breaches of confidentiality by releasing confidential data to third parties, and the release of records to governmental agencies for investigative purposes.

The basic law that protects our privacy is the Fourth Amendment to the United States Constitution, which mandates that people have a right to be secure in homes and against unreasonable search and seizure. In addition, many laws have been enacted to protect the individual from having damaging information stored in computerized databases.

E. *Issues of Adjudication and Regulation*

Traditionally, prosecutors face a great deal of uncertainty when they attempted to use existing criminal statutes to prosecute offenses. Within the last few years, this has changed with the addition of computer crime statutes to many state and federal codes.

Computer crime laws can be seen as a generalized reaction to many types of computer crime. The goal of these laws is to define that acts will be punished, in the hopes that this will deter computer crime. Some of these acts include trespassing into a computerized system, the invasion of privacy of an individual, theft of money, service, data or programs from a computerized system, and data alteration or destruction. Computer laws also prevent or deter computer related fraud and the misuse of computerized information.

That is to say, the law provides compensation for injuries and, hopefully, deters wrongdoers by the smooth and efficient operation of the legal system. Generally, the law does not provide a remedy if no injury has occurred; it as a shield through its deterrent effect and not in a proactive manner. Where it is vital that the injury does not occur, then the physical and environmental controls described elsewhere in this text must be used as additional barriers against the wrongdoer. On the other hand, after a wrongdoer has compromised the physical or environmental security arrangements, the law is frequently the only tool available to the information security specialist to minimize the injury already done and to deter, as far as is possible, future wrong doing.

II. LAWS AS TOOLS FOR COMPUTER SECURITY

A. *Privacy Laws and Legislation*

Loss of privacy is a danger that continues to grow with the proliferation of computerized data banks. The computer's ability to collect, store and manipulate vast amounts of data, and its ability to retrieve selected items from these data banks, almost instantaneously allows the collection and distribution of personal information that can affect one's privacy. One of the primary defenses against the loss of individual privacy is the enactment of legislation by national and state legislatures. The basic concern of privacy legislation has been the control and protection of information on or about individuals.

Privacy protection laws have been passed in most developed countries. Early in 1970, the U. S. introduced the Fair Credit and Reporting Act that governs the processing, access, and disclosure of credit information. The U. S. Privacy Act of 1974 and the Canadian Privacy Act of 1975 are examples of laws that mandate protection of individual privacy. Other countries also have enacted laws related to individual privacy including the Swedish Data Act of 1973, the German Federal Data Protection Act of 1977, the French Act on Data Processing of 1978, the Danish Acts on Private Registers and the Austrian Federal Data Protection Act of 1978. At the international level, the OECD Transborder Data Flow Guidelines address the topic of the flow of information across international borders, perhaps to jurisdictions where privacy laws may differ from the originating venue.

B. *Intellectual Property Laws*

Intellectual property relates to secrets, names, ideas and other similar concepts. The creator of this type of property -- whether it is a book, a play, a program, or a musical composition -

- has certain rights to this property. Four bodies of intellectual property law protect different aspect of these ideas and their practical applications.

1. **Trade Secrets Law**
   A trade secret protects something of value and usefulness. This law protects the unique and secret aspects of ideas, known only to the discoverer or his confidants. Once disclosed the trade secret is lost as such and can only be protected under one of the following laws. The application of trade secret law is very important in the computer field, where even a slight head start in the development of software or hardware can provide a significant competitive advantage.

2. **Patent Law**
   A patent can protect the unique and secret aspect of an idea. It is very difficult to obtain a patent compared to a copyright (please see discussion below). With computer software, complete disclosure is required; the patent holder must disclose the complete details of a program to allow a skilled programmer to build the program. Moreover, a United States software patent will be unenforceable in most other countries.

3. **Copyright Law**
   Copyright law provides a very significant legal tool for use in protecting computer software, both before a security breach and certainly after a security breach. This type of breach could deal with misappropriation of data, computer programs, documentation, or similar material. For this reason the information security specialist will want to be familiar with basic concepts of to copyright law.

   The United States, United Kingdom, Australia, and other countries have now amended or revised their copyright legislation to provide explicit copyright laws to protect computer program. Copyright law in the United States is governed by the Copyright Act of 1976 that preempted the field from the states. Formerly, the United States had a dual state and federal system. In other countries, such as Canada, the courts have held that the un-revised Copyright Act is broad enough to protect computer programs.

4. **Trademark Law**
   The name given to the software is often as important as the protection of the software itself and must be protected. Trade names for well known products have gained great value as their commercial recognition has increased. Trademark laws exist under both state common laws and federal status. Trademark rights arise upon ‘first usage’ of the trademark in commerce.

   Trademarks should be used to protect the names of any software packages. Simply using a trademark gives one common-law rights to continue using it. If the trademark is registered with the Patent and Trademark Office the holder has the rights to use the trademark anywhere business is conducted.

C. *Federal Laws*

Federal laws, such as the Privacy Act of 1974 and the Foreign Corrupt Practices Act, were used to combat computer crime during the late 1970’s and early 1980’s. The Ribicoff Computer Crime Bill of 1978 was used as a basis for many of the first state computer crime laws as well as Federal legislation. During 1984, Congress enacted the first federal provisions, within several bills, specifically outlawing certain types of computer abuse. These provisions prohibited the unauthorized use of computers in three areas:

- They made it a felony to access a computer to obtain classified military or foreign policy information.
- They prohibited access to a computer to obtain financial or credit information without authorization.
- They made it a misdemeanor to access a federal computer to modify or destroy data.

During 1986, the 99th Congress allowed for modification of Title 18 of the United States Code, which includes Section 1030 (fraud and related activity in connection with computers). The Federal Computer Crime Statute, as mentioned above, was put in place in 1984 and provided criminal penalties only for stealing national security related data or for trespassing into government computers and computerized information of individuals' credit histories. The 1986 modifications of this statute made it clear that acts of simple trespass into government computers are punishable, authorized prosecution of those who traffic in compute passwords and strengthened the 1984 law by expanding protected data beyond federal databases to those holding government - related data such as banks or other financial institutions.

The Computer Security Act of 1987 was the primary computer security legislation of the 100th Congress. The legislation provides for a computer standards program within the National Bureau of Standards (now the National Institute of Standards and Technology [NIST]). This act states that NIST shall be responsible for developing standards and guidelines related to security and privacy for federal computer systems that store and process "sensitive" information. NIST is also tasked with issuing guidelines for training awareness, that must be followed by federal agencies. While NIST will set the standards for the area of "sensitive" information, the Department of Defense will retain jurisdiction over systems with classified information that require protection under Executive Order 12356.

D. State Statutes

The first ten states to adopt computer crime legislation were Arizona, California, Colorado, Florida, Illinois, Michigan, New Mexico, North Carolina, Rhode Island and Utah. Today some 48 states have passed computer crime legislation. These laws usually define computer crime in great detail including such terms as 'theft of services', 'criminal use of the computer', 'deceiving a machine', 'computer fraud', 'computer program', 'computer network', etc. Many of the state laws also specify the maximum fines and punishments. For example California's computer crime law specifies a maximum $10,000 fine for accessing a computer for extortion. The Louisiana law specifies that an offender may be fined not more than $10,000 and imprisoned for not more than five years.

The Maryland computer crime law concentrates on access to a computer, computer network, computer software, computer control language, and computer databases. Fines are not to exceed $1,000 and imprisonment not to exceed three years. It appears that the Maryland legislature does not think unauthorized computer access is a very serious matter. Damage or destruction of hardware is designated as an offense in the Minnesota law. Maximum fines are specified at not more than $10,000. The Montana law attempts to define the value of the electronic impulses, electronically produced data, computer software. Denial of computer use is defined as an unlawful act in the Nevada law. New Jersey law defines alteration and destruction of data as a crime. Extortion is mentioned in the North Carolina law. The Oklahoma law specifies a maximum fine of $100,000. Washington law uses the term computer trespass rather than access. The theft of trade secrets and intellectual property are addressed in the Wyoming law. Connecticut law has provisions that protect the privacy of individuals including the elimination of governmental immunity.

These laws, plus additional ones that are being added each year, attempt to make computer related crime less attractive to individuals and groups who are willing to risk fines and imprisonment. For example, thirteen state legislatures proposed some 21 pieces of computer crime legislation during their 1987 sessions and during the 1988 sessions some seven states proposed legislation. These bills propose new definitions of computer crime, revised definitions of the terms used in existing laws, enhanced penalties, proposed authorization for certain agencies to conduct computer crime investigations and propose compensation procedures for victims of computer crimes.

For example, a proposed California law would greatly broaden the state's authority to prosecute computer crimes. The bill has been criticized as being too harsh. Under this bill punishment for unauthorized access to a computer would depend not only on the dollar value of the computer time used but also on the expense of assessing and repairing damage to the system. One feature of the bill removes the burden of proving malicious intent on the part of the defendant. It also allows the seizure and confiscation of items seized as the result of a warrant or arrest. These items may be destroyed or distributed to a public entity or nonprofit corporation. An Illinois Senate bill also provided for forfeiture of any moneys, profits or proceeds acquired directly or indirectly as the result of a computer crime.

Several bills refine or enhance existing laws. An Idaho Senate bill defined computer crime within the definitions of trade secrets. The Massachusetts legislature is considering a bill that establishes a commission to determine and review the adequacy of current laws defining computer crime. Both New Mexico and North Dakota passed legislation which further defines or redefines computer crime and computer fraud. The Utah legislature has passed legislation to provide for compensation to the victims of computer crime.

The Texas State Legislature passed legislation related to the intellectual property policies of institutions of higher education. One of the matters addressed in these bills was disclosure of scientific and technological developments including computer software. This act is a basis for the control and protection of computer software developed at institutions of higher education in Texas.

E. DPMA Model Computer Crime Bill

Apparently, at the state level, legislation is not uniform nor is it consistent. Work needs to be done to strengthen current and proposed legislation at the state level. With this objective in mind, the DPMA has taken an active interest in this effort by calling for the improvement of existing computer crime laws. It has proposed and drafted a "Model Computer Crime Act." The model act establishes civil procedures for redress of computer crime victims. The DPMA model act also proposes forfeiture of property, guidelines for what evidence will be considered in a computer crime case (rules of evidence), a good definition of computer crime, suggested punishments (including increased penalties for repeated violations) and suggestions for jurisdiction. Jurisdiction is a significant problem for the courts since the computer criminal may reside in one state or country while committing a crime in another via data communication systems.

Security practitioners must keep abreast of current legislation even though the impact of these laws on the prospective perpetrator of a computer crime may not be great. A review of the literature shows that most researchers believe that the probability of being convicted of a computer crime is low and that when convicted the punishments are nominal. Strengthening our existing laws can have a positive impact deterring would-be perpetrators of computer crime.

III. LAWS AND LEGISLATION AS OPTIONS TO CONTROL COMPUTER CRIME

A. *License Agreements*

A common practice in the computer industry is to license the use of software rather than sell it outright. This is particularly true with mainframe software and much of the microcomputer software. The law related to license agreements is complex and of interest to the computer security specialist since a company's liability could be substantial if infringements occur. A license agreement is a contract that permits the licensee to exercise owner's rights under certain conditions and constraints for a fixed period. The extent of those rights varies from one license to another. Under a license agreement, the right to use computer hardware or software is often limited and defined. These constraints may include number of hours of use per period, the location of use, limits on the number of copies that may be made, limits on the number of terminals that can be used and similar items. Obligations of secrecy are often imposed as part of the license agreement.

A license agreement is also a device for legally forbidding copying of computer programs. Under a license agreement, the developer remains the owner of the program. The publisher, the owner of the license, is only allowed to market the program under certain constraints imposed by the license agreement. When we pay a software vender for a computer disk and written documentation, we do not actually purchase the software. Instead, we have only paid for a license to use the software. We only have the right to use the software as specified in the license agreement. A distinction must be made between the purchasing of software and obtaining a license to use software.

A number of actions should be taken to ensure the owner's proprietary rights. Owners should limit the use of their software to certain purposes, times, and conditions so that its confidentiality is maintained. Instead of selling an unlimited right to copy a program, the owner will ordinarily specify the number of copies that the purchaser can make. The matter of royalties should be agreed upon between the developer and the licensee. The license should clearly allocate the legal responsibilities of the developer and licensee so that should any liability for infringements or program defects occur, a specify procedure can be followed to resolve the dispute.

There are a number of forms of license agreements, including box-top and shrink-wrap license agreements. These are agreements that are put on the outside of the package containing the software. They may be printed on the box or be held in place by a transparent plastic package wrapping. Typically, agreements warn the purchaser that they are only acquiring the license to use the program and specify clearly the rights of the licensee. Upon opening the package the licensee has accepted the terms of the license agreement.

B. *Intellectual Property Laws, (Trade Secrets, Patents, Copyright and Trademarks)*

A trade secret is any information, process, or idea that a company considers confidential and it is not generally known in the industry. This secret gives the company a competitive advantage over others. Its existence is simply based on the obligation of confidentiality among the parties involved. Unlike the copyright law, which is discussed below, it can only offer limited protection related to ideas such as a program, formula, or device.

Trade secrecy is probably the simplest and the most widely used method to protect software. Owners of a trade secret have exclusive rights to its use and they may license another person to use their innovation for some specified purpose. Under no circumstances should the licensee violate the agreement by disclosing the secret to unauthorized person or use it for unauthorized purposes.

The trade secrets law may be used to protect object code as well as source code. Unlike the copyright, it is not a federal law. So, it is practicable in most situations to protect source codes by the trade secrets law and the object code by the copyright law. If object code is only protected as a trade secret, it can only be used as a secret and it cannot be mass marketed. Theoretically, a seller can require every user to sign a nondisclosure agreement when they acquire software. However, it would be inconvenient and unnecessary. Thus, copyright is often viewed as a better alternative when software is sold.

The trade secrets law may not pose any legal restrictions in some cases. People may obtain software or other items covered by trade secrets agreements accidentally or intentionally without signing a nondisclosure agreement. Once the secret gets out, it is opened to others forever. Another problem is 'independent discovery' that means other people may develop the same program independently without being legally responsible for any trade restriction. "Reverse engineering" is legally the same as independent discovery.

In many instances, trade secrets protection is preferable to copyright and patent protection. There is too much confusion in the legal profession regarding patent and copyright protection of software for developers to feel justified in entrusting their competitive advantages to those two forms of protection. With the patent and copyright, developers are required to make the development public as a perquisite for protection. Since trade secrets protection does not require any registration with government agencies, it is often viewed as a simpler form of protection. Protection exists once creation begins and it is quite a natural practice for a developer to protect his innovation by keeping it confidential.

Using trade secrets protection has a number of drawbacks. First, a trade secret exists only as long as it is still a secret. A developer may be required to go to great lengths to establish and ensure the continued confidentiality of the innovation. Second, developers cannot restrict their competitor from discovering the new idea independently. Third, widespread trade secrets protection may tend to stifle technological development since it encourages jealous safeguarding of software improvements rather than the free interchange of new ideas.

As mentioned above the use of the patent is impractical for the protection of software and is certainly a viable alternative for hardware protection. While there may be an occasion when a program might be patentable, confusion and uncertainty in the law creates doubt that a patent would be feasible. The costs of a patent are prohibitive compared to the cost of a copyright.

A copyright owner has the exclusive right to reproduce his work. Copyrights can also be obtained if an author transfers the right to a third party. This applies to software as well as literature and art. Under the Copyright Act, a person who copies an idea for a program and not the actual code should not have infringed on the author's copyright. Unfortunately, this look and feel doctrine has been supported by only a few cases in the courts. These cases involve defendants who stole the code of the plaintiff and wrote the same program in a different language.

Microcomputer software presents a particular problem since many individuals are involved in the use of this software. Section 117 of the copyright laws, specifically the 1980 amendment, deals with a law that addresses the problem of backup copies of software. This section states that users have the right to create backup copies of their software. That is, users may legally create a backup copy of software if it is to be held in archive. Many software companies provide a free backup copy to users that precludes the need for to users purchase software intended to defeat copy protection systems and subsequently create copies of their software. If the software purchased is actually leased, you may in fact not even be able to make backup copies of the software. The distinction between leasing and buying is contained within the software documentation. The copyright statement is also contained in the software documentation. The copyright laws regarding leased material state that the leasor may say what the leaseholder can and cannot do with the software. So it is entirely up to the owner of the software as to whether or not users may make backup copies of the software. At a time when federal laws relating to copyright protection are evolving, several states are considering legislation that would bar unauthorized duplication of software.

The software industry is prepared to do battle against software piracy. The courts are dealing with an increasing number of lawsuits concerning the protection of software. Large software publishers have established the Software Protection Fund to raise between $500,000 and $1 million to promote anti-piracy sentiment and to develop additional protection devices.

C. *Employee Non-Disclosure Considerations*

A non-disclosure agreement is an established form of agreement between employees and a company in which an employee agrees not to disclose trade secrets or other confidential information owned by the company to any unauthorized person. It provides a legal basis for future prosecution of employees who breach security. Thus, employers retain their ability to hire or fire employees and also maintain their legal right to protect their trade secrets. Some of the significant elements in non-disclosure agreements include: an indication and definition of which trade secrets are involved, an obligation for the agreement to continue beyond termination of employment, restraints on duplication of material and exit review procedures when an employee terminates employment.

In fulfilling employees' obligation under this agreement, employees promise not to disclose company trade secrets unless authorized in writing by the company. This agreement should remain in force even after employment has been terminated. Upon termination of employment the employees agree to surrender to the company all notes, records, and documentation that was used, created, or controlled by the employee.

A non-disclosure agreement should stress that an employee should take his or her involvement with trade secrets seriously and must legally bind the signer from disclosing trade secrets. Should the signer disclose the secrets to others, he cannot legally make use of it without facing the possibility of an injunction.

D. *Contracts*

Software development contracts can play a contributing role in any security program. The subject of buying and leasing software and hardware cannot be explored without some basic knowledge of contract law. Often the user rushes into the contracting stage by signing the supplier's standard form of contract often called the sales order. This is done without documenting claims made by the salesman and without realizing that the sales order is legally binding. If the purchaser is to protect himself fully, he or she must include certain clauses in these contracts.

Room does not allow a complete discussion contracts except for some of the important clauses that are of particular interest to the computer security specialist. The interested reader should refer to one or more of the references listed at the end of this module.

Written contracts should always designate a time frame or timetable in which the hardware is to be installed or software completed. Specify details when various parts of a program shall be completed and tested or likewise when hardware components shall be installed. Outline in detail the functional specifications for performance criteria and interface specifications. Include a list of authorized signatures of both parties to the contract. Specify the method and timing of payments in detail. Include definitions of terms that require clarification. Allocate responsibilities between the two parties involved to include what is expected of each. If software is to be developed, a detailed description of the software must be included. The user and supplier must agree that both parties will use all the Uniform Commercial Code (UCC) rights, duties, and remedies. Include some form of progress reporting system for hardware installation or the programming of software, plus a warranty that the products produced or purchased will perform according to specifications; provide for program maintenance and provide for access to source code via such agreements as a source code escrow.

Detailed specifications are very important in any contract. Put in writing exactly what the program is to do or how the hardware is to perform. Since the user is the one who determines the specific adequacies of a product, the more detailed the contract, the better the user position. The user and seller must agree on the form and level of performance acceptance tests for hardware or software. These tests should be directly related to the previously mentioned functional specifications. The best solution for obtaining functioning programs is to use care in selecting a programmer or software house that is competent, reliable and financially sound.

For protection, users should formulate a payment schedule so that a payment is made as each phase of installation is completed, tested, and operating properly. Should the project be delayed, the supplier will be responsible for any loss to the user. This encourages suppliers to meet time schedules and provides some bargaining leverage between the user and the supplier of the hardware or software. Custom-designed programming is more likely to develop problems and take longer to debug. Therefore, users should take this possibility into consideration when negotiating with the contractor.

Make provisions for maintenance of hardware and/or software. Include up-time commitments for hardware and performance specifications for software. Agree upon the replacement procedures for non-functioning hardware or software "Lemons" needs to be agreed upon.

E. *Warranties for Software and Hardware*

Consider comprehensive warranties for any hardware or software leased or purchased an important element in any security program. As pointed out above, different rights and obligation arise from the sale or lease of computer software and hardware. The sale of a product gives rise to certain warranties by the seller. A warranty is a promise that a particular statement is true, that the software or computer hardware will work as specified. The genesis for warranties is the Uniform Commercial Code (UCC) which divides warranties into two types: express and implied. Few express warranties are used in the sale of computers or software. Implied warranties, which imply that a product is fit and proper for the function advertised, are very common.

Under the UCC, an express warranty is an affirmation or promise of product quality to the buyer and becomes a part of the basis of the bargain. Promises and affirmations made by the software developer to the user about the nature and quality of the program can also be classified as an express warranty. Programmers or retailers possess the right to define express warranties. Thus, they have to be realistic when they state any claims and predictions about the capabilities, quality and nature of their software or hardware. They should consider the legal aspects of their affirmative promises, their product demonstrations, and their product description. Every word they say may be as legally effective as though stated in writing. Thus, to protect against liability, all agreements should be in writing. A disclaimer of express warranties can free a supplier from being held responsible for any informal, hypothetical statements or predictions made during the negotiation stages.

Implied warranties are also defined by the UCC. These are warranties that are provided automatically in every sale. These warranties need not be in writing nor do they need to be verbally stated. They insure that good title will pass to the buyer, that the product is fit for the purpose sold, and that it is fit for the ordinary purposes for which similar goods are used (merchantability).

Teaching Considerations

A. SUGGESTED SCHEDULE:

The following sample module plan is based on the offering of three to nine hours of lectures with outside lab time and some homework.

1. **The Underlying problem.. 1 - 2 hours**
2. **Laws as tools for computer security.. 1 - 3 hours**
3. **Laws as legal options for control .... 1 - 4 hours**

As an alternative a one hour lecture could be presented discussing only topic II.

B. CASE STUDIES/EXAMPLES

The Computer/Law Journal, which can be found in most major libraries is a very good source of examples and case studies.

C. HOMEWORK AND LAB EXERCISES

Ask students to complete a brief two or three page summary of current articles related to computer law. Trade publications such a Datamation and Computer World often have articles that can be used as cases. Ask the advanced student to review court cases.

Bibliography

Becker, L. G., *Computer Abuse and Misuse: Assessment of Federal and State Legislative Initiative*, Institute of Defense Analyses, 1801 N. Beauregard Street, Alexandria, Virginia, IDA Paper P-1798, 1984.

This publication includes an overview of computer abuse issues, Federal legislation through 1984, state computer abuse statues and the implication for the DOD.

U.S. Congress, “The Security Act of 1987,” PL-100-235.

This law describes the policy of the Federal Government regarding computer security. Among other things the law covers the identification of sensitive systems, the development of a security program and plan, and the need for training of all users, developers and operations associated with a system.

“Model Computer Crime Act,” Data Processing Management Association, Park Ridge, IL, 1986.

This model act incorporates the establishment of civil procedures for redress of computer crime victims. The DPMA’s model act also proposes forfeiture of property, guidelines for what evidence will be considered in a computer crime case (rules of evidence), a good definition of computer crime, suggested punishments including increased penalties for repeated violations and suggestions for jurisdiction.

Davis, G. G., *Software Protection, Practical and Legal Steps to Protect and Market Computer Programs*, Van Nostrand Reinhold, New York, 1985.

An academic discussion of intellectual property rights, copyright, unresolved problems with copyright, software warranties, export controls, and infringement remedies.

Mandell, Steven L., *Computer Data Processing, and the Law*, West Publishing Company, Minnesota, 1984.

This book has been designed especially for the functional aspects of data processing management.

Hagelshaw, R. Lee, *The Computer User's Legal Guide*, Chilton Book Company, Pennsylvania, 1985.

This text provides a good overview of the most common legal aspects of interest to the computer users in a manner that can be understood.

Remer, Daniel, *Legal Care for Your Software*, A Nolo Press Book, United States, 1984.

This book is designed as a legal guide for software writers and publishers. It clearly describes the legal rules that relate to developing and marketing computer software.

Isshikki, Koichiro R., *Small Business Computers, a Guide to Evaluation and Selection*, Prentice-Hall, Englewood Cliffs, N.J.,1982.

A comprehensive text containing a detailed chapter on how to avoid computer contracting pitfalls.

S Y S T E M S E C U R I T Y

Revised August 1990
Revised May 1995
Revised February 2001

Corey D. Schou, Ph.D.
National Information Assurance Training and Education Center
College of Business
Idaho State University

Description:
This module addresses mainframe security considerations. It will define the advanced requirements for security and the criteria on which satisfaction of those requirements can be judged. Hardware, software, firmware, and procedures are considered as mechanisms to protect a system appropriately. The process described starts by defining of the sensitivity of a system and moves through techniques of establishing criteria and evaluating the degree to which the criteria are met.

The module is the first of the senior level modules and addresses mainframe security considerations. The module defines advanced requirements for security and the criteria on which satisfaction of those requirements can be judged. Hardware, software, firmware, and procedures are considered as mechanisms to protect a system appropriately. The described process starts by defining the sensitivity of a system and proceeds through establishing criteria and evaluating the degree to which the criteria are met.

SYSTEM SECURITY

OBJECTIVES:

The objective of this module is to provide an understanding of the techniques of defining and evaluating mainframe system security requirements.

LEARNING OBJECTIVES

Upon completion of this module, the student should be able to:

- determine the sensitivity of a system;
- recognize the difference between criticality and sensitivity;
- determine the corporate impact of loss;
- relate system sensitivity to security requirements;
- determine criteria to be met to satisfy security requirements;
- recognize and evaluate the levels of security of systems.

PREREQUISITE:

The modules "Introduction to Computer Protection" and "Security Fundamentals" are appropriate. In addition, knowledge of computer systems design and requirements would be beneficial. This module should be incorporated at the upper division of undergraduate work so that the student will have achieved a level of maturity that will enhance participation.

Topic Outline

I. Overview
    A. Definitions
        1. Sensitivity/Criticality
        2. Security Levels
        3. Accreditation/Certification
    B. Background
        1. Threats and Vulnerability
        2. Computer Security Act of 1987
    C. Management Responsibilities
II. Systems Sensitivity
    A. Criticality
        1. Business Impact
        2. Revenue Losses
        3. Embarrassment
        4. Potential Legal Problems
    B. Sensitivity
        1. Privacy
        2. Trade Secrets
        3. Planning Information
        4. Financial Data
    C. Source Of Sensitivity Information
        1. MIS Department
        2. Users
        3. Management
    D. Levels Of Sensitivity
        1. Military
        2. National Computer Security Center
        3. Commercial
III. Security Requirements
    A. Security Policy
        1. Intent (As It Relates To Sensitivity)
            a. Access To Information
            b. Destination Of Information
        2. Laws
        3. Regulations
        4. Company Policy
        5. Mandatory Security And Discretionary Security
        6. Responsibilities
    B. Accountability
        1. Individual Identification
        2. Authentication
        3. Audit Capability
    C. Assurance
        1. Architecture
        2. Integrity
        3. Testing
        4. Specification/Verification
        5. Facility Management
        6. Configuration Management And Control

7. Disaster Recovery Or Contingency Planning
8. Compliance

IV. Levels of Security
  A. Related To Sensitivity
  B. Extent To Which Requirements Are Satisfied
  C. Cost/Benefit Analysis
  D. Management Decision

V. Data Life Cycles
  A. Retention Policy
  B. Destruction Policy

VI. Sample Protection Plan
  A. System Description
  B. MIS Security
  C. Communications Security
  D. Information Security
  E. Personnel Security
  F. Physical Security
  G. Contingency Plans

Annotated Outline

I. OVERVIEW

A. *Definitions*

This section is intended to introduce the student to System Security and to provide the definition of specific terms that will be used throughout this section: criticality addresses the impact of computer capability loss; while sensitivity represents the value of the integrity and protection of the information in the system. These factors together, define the importance of a computer system, and the data that it contains, to the organization.

These factors also define the level of protection or security that is cost justified for a specific system. Fundamentally, the implementation of security countermeasures results in the certification by a knowledgeable authority that adequate measures are in place and includes the ultimate approval or accreditation of the system. The sensitivity of the system and the organization's culture determines the level of formality of this process.

B. *Background*

Examine the reasons for increasing levels of security by briefly discussing current threats, both natural and man made, that have been reported in the news media. Use these events to illustrate the vulnerability of computer systems in terms of the basic concepts of system protection. The Computer Security Act of 1987 demonstrates the role that the Federal Government plays both in defining basic concepts and articulating current thinking on the subject. Stress the responsibilities for the following tasks:

- Identifying sensitive systems
- Developing a security program and plan, and
- Training appropriate people concerned with both development and operation of systems.

C. *Management Responsibility*

Responsibility for computer security is broad based: people in all organizational elements must take part. Management must direct and coordinate this effort and provide the impetus to make it work.

II. SYSTEM SENSITIVITY

First determine what systems are sensitive and the extent they must be protected. This includes identifying sensitive data.

A. *Criticality*

Evaluate criticality in terms of what would be affected if the system were to become unavailable. First, divide the system into sub-elements (i.e., applications) that are related to users or business functions. Then evaluate each application to define the impact on the user if computer support was lost. Such factors as the effectiveness of the particular function, additional cost of doing business, lost revenue, possible legal problems, and the effect of the loss on the image of the organizations.

B. *Sensitivity*

Sensitivity analysis measures the impact of a non-authorized person gaining access to the information, or of data being altered in any way. Most importantly, private personal data should not be disclosed without specific authorization. Other sensitive areas include trade secrets, formulas, financial data and company planning information that may be of significant value to competitors.

C. *Source of Sensitivity Information*

Do not consider the MIS group a reliable source of criticality and sensitivity information. Too often the MIS group reacts to an individual or group that most quickly to complains in the event of system degradation. The quickness of the complaint may not necessarily be representative of the real importance of these data to the company. The best initial sources are the users of the MIS output. They can best express impact on the operation and potential costs, thus when this information is validated by management the real importance to the organization is captured. This is the foundation for systems security -- validity must be guaranteed.

D. *Level of Sensitivity*

The military, expresses sensitivity of systems through classification such as top secret, secret, confidential, and unclassified. The recent introduction of “unclassified but sensitive” was a reaction to privacy requirements.

The National Computer Security Center, in its Trusted Computer System Evaluation Criteria standard, identifies four divisions of security. Level “D” is the lowest; no security is required. Each higher division represents a major improvement in the confidence one can place in a system for the protection of information. The “C” level is discretionary control, in which identifiable sections of a system are protected, as appropriate, to the information in the section. The “B” level is defined as Mandatory Control in which all data are protected. Although some data may be more easily accessed than others the necessary controls are present. The “A” level is the highest - it represents formally verifiable protection and is the most comprehensive security available.

Commercially, various categorization schemes are employed. Commonly, such terms as highly critical, critical, important, and routine are used. The actual names used are unimportant as long as they are used consistently. The key factor is that levels are defined so they can be used to identify the extent to which security measures should be applied to the system.

III. SECURITY REQUIREMENTS

Security requirements may be divided into three general areas: security policy, accountability, and assurance. Each area represents what may be done to control, through specific security features, over information access so that only authorized individuals or processes may read, write, create, or delete the information.

The satisfaction of security requirements may be accomplished with hardware, software, firmware, procedures or any combinations of these elements. The extent to which the requirements are satisfied is related to the sensitivity of the system and is defined through a cost/benefit analysis that will relate the marginal cost of the measure to the previously defined level of sensitivity.

A. *Security Policy*

Security policy must be explicit and well defined. This is a statement of intent regarding access and distribution of information. This policy may be positively or negatively formulated, - “all appropriate individuals will have easy access to the information they require,” or “no unauthorized individual may have access...” The policies must be explicit enough so that specific interpretations can be made and must also be distributed to the appropriate individuals.

A security policy should reflect any laws, regulations, or basic company policy. Particular attention must be paid to the privacy of individual personal information. Failure to create a valid and complete security policy could put any organization at great risk.

The policy should state whether discretionary or mandatory control is to be employed and the extent to which formal verification is to take place. Most importantly, the policy must clearly delineate the responsibilities of all those involved. All factors should be related to the level of sensitivity.

A list of subjects covered in the policy area includes:

- Responsibility/Authority
- Access Control
- Discretionary/Mandatory Control
- Marking/Labeling
- Control of Media
- Import & Export of Data
- Security Levels
- Treatment of System Outputs

B. *Accountability*

The system must assure individual accountability both for access to data and use of system capability. There must also be a way to audit transactions. This involves three basic elements: individual identification, authentication, and audit.

Individual Identification refers to the ability to recognize uniquely anyone accessing the system. This can be determined at any level a policy requires. Many access control systems group individual users so that the same privileges (i.e., access to specific data or functions) are granted to several individuals. These privileges may also be related to location, time of day, or other criteria that in turn relate to the level of security required. For example, in a hospital information system, doctors may be able to access data about a patient from any location while nurses may only be able to access data about medication for specific patients from specific stations. The level of individual access authority control should relate directly to sensitivity levels previously defined.

Authentication refers to techniques available to assure that individuals identified are who they represent themselves to be. The most common form of authentication is the use of passwords, but there are other techniques. Authentication techniques fall into three categories: what someone knows (passwords, encryption keys); what someone possesses (smart cards, electronic keys); or some personal characteristic (biometrics -- fingerprints, hand geometry, retina patterns). In the sequence of reliability and ease of use, what someone knows is easy and inexpensive to implement. What someone possesses is also easy to use but more expensive and more reliable because of the greater difficulty to compromise. Human error, however, is more highly probable when relying on what someone knows and what someone posses. Passwords, and the use of encryption methods, require keys. Management of passwords and keys determines the reliability and security of a system.

Audit capability refers to the capability of authorized personnel to track actions taken by individuals. The system must provide authorized personnel with the capability to track actions taken by individuals. The granularity of these tracking mechanisms relates to sensitivity. The higher the level of sensitivity, the more detail should be available in the auditing system. The authorized user should be able to manipulate easily the system so that data can be selected as needed.

C. *Assurance*

Assurance refers to the guarantee of correct policy interpretation, the integrity of the system, and the effective operation of the system. The degree to which the subjects listed below are addressed pertains to the security level of the system. The elements contained in the assurance category are:

- Architecture: Specify the security relevant aspects and clearly identify how they are treated.
- Integrity: Both system and data integrity should be addressed. The analysis should include what checks are made, the frequency, and the impact of failure.
- Testing: No system can be considered secure if adequate testing has not been done. The test should be well planned and structured and evaluation should be directed toward making improvements.
- Specification/Verification: To establish the security of a system, it is necessary to know what the system should be doing and determine how well it accomplished its functions. It is impossible to define security requirements if the function of the system is not known.
- Facility Management: This addresses physical access control and operational actions, such as policy change, program implementation procedures and other actions that relate to the manner in which the system is implemented and operated.
- Configuration Control: This is relative to the certain knowledge of the contents of hardware and software at any given moment.
- Disaster Recovery or Contingency Planning: This element of system security has two distinct parts -- what must be done during normal operation and what must be done in the event of emergency. Effective backup data creation and storage are as important as the identification of a backup concept and storage facility. The intention of this discussion is not to address disaster recovery fully, but to ensure that it is considered.
- Compliance: The identification and treatment of violations to established policy is important. Both the mechanism to identify violations and the response to violations must exist and be enforced. Objective review must be made to ensure that security procedures are being complied with.

IV. LEVELS OF SECURITY

The security measures taken need to relate to the sensitivity of the system. All systems are, or can be, secured to the necessary level by application of the appropriate principles discussed. One of them, password protection, may be very simple and not managed in detail or it may be very complex and rigid in nature. An individual may be required to know several passwords to access increasingly more sensitive data. Each requirement should be addressed - even if the answer is that its use is unnecessary for the specific system involved.

Evaluation of the extent to which security measures should be applied can be done with Cost/Benefit analysis. It should never cost more to implement a countermeasure than it is worth. The process is briefly discussed here, it is only necessary for the student to understand that cost/benefit analysis will relate the value/cost of possible losses to the cost (dollar and organizational) to accomplish a specific protective action.

It should be emphasized that these are management decisions. They should not be defaulted to system developers or designers but should be thoughtful and intelligent decisions made by management based on knowledge and information.

V. DATA LIFE CYCLE

All data within an organization have a finite life cycle. Retention of this data beyond their useful life exposes the organization to unnecessary risk of compromise or disclosure. It is therefore important that the organization have both a retention and destruction policy.

A. *Retention Policy*

The retention policy should be realistic and take into account the importance of the data or information to the organization in the future. Files should be marked at the time of their origin for automatic destruction. Files which are company private and do not have an automatic destruction date should be reviewed by the originator and by a company security office for review before release.

When company private files are reviewed and it is determined that they are no longer needed, The originator and all users should be notified that the status of the data or information is to be changed. A reasonable time might be specified before destroying the files.

B. *Destruction Policy*

Once it has been determined that the files have outlived their usefulness, they should be destroyed. The following is a sample procedure that one may use for this destruction.

- Removable media shall be overwritten (if appropriate) with a binary pattern. One method for overwriting is to overwrite all storage locations with either all 1's or 0's three consecutive times.
- Removable media may be erased by exposing the recording surface to a permanent magnet having a field strength at the recording surface greater than the magnetic intensity that recorded the material on the media. (e.g., A degausser)
- Non-removable media shall be checked immediately before beginning the overwrite procedure to ensure that malfunctions do not occur that will prevent the classified information from being effectively overwritten. The

manufacturer's specifications shall also be reviewed to determine whether the overwriting procedures are valid for the particular storage media. Some devices may have unique properties that would prevent the complete erasure of classified data without destroying the storage device. Once it is determined that overwriting is appropriate, all storage locations will be overwritten with a binary pattern as described above.

- Non removable media containing company private material that is mechanically or electronically defective and cannot be repaired in a secure facility should be destroyed in accordance with the regulations defined by the company policy.
- It should be noted that the act of formatting a disk does not remove the data and therefore does not meet the definition of declassification.
- Media shall be destroyed by burning, shredding or any other method that assures complete destruction.

VI. SAMPLE PROTECTION PLAN

The following is a sample protection plan for an organization. It should be customized to meet the requirements of the organization.

A. System Description -- This should contain:

- The physical location of the equipment. For example, the Steam Whistle 3000 machine is located in room 941 (9th floor) of building 18 (S. Caesar Lane and A. E. Neumann Drive) in a technical area with limited access.
- Types of data and information -- For example, the SW-3000 processes data related to production of widgets and personnel files.
- Classification level -- For example, the highest level classification of data or information that is to be processed is "B" level that is defined as Mandatory Control.
- Duration and Importance of MIS Activity -- For example, The requirement for the Steam Whistle -3000 to process "B" level data will continue for an indefinite period.
- Equipment Location -- The majority of the hardware is located at the facility described in location 1.A; however, there are also disks on the eighth floor..
- Equipment Description by Name and Model Number -- self explanatory
- Security Officers -- For Example

Security Officer	Jim Frost	555-1212
Alternates	Sue Bond	555-1312
Alternates	Dee Jensen	555-0212

- Data Processing Terms -- The data processing terms used in this security plan are consistent with those appearing in the company standards manual.
- System Integrity Study -- The integrity study will contain the access needs.

B. MIS Security

This should include all aspects of system security such as access methods and user control. Additionally risk analysis and audit review information should be considered in this portion of the study.

C. *Communications Security*
This should include all aspects of communication security with the outside world. The Radio Frequency Interference (RFI) control requirements and network access precautions should be addressed in this portion of study.

D. *Information Security*
This should include all aspects of system security responsibility of each user and how the system keeps user information separate. Details on projected percentage and level of information type should also be included. Finally risk analysis and audit review information should be included in this portion of the study.

E. *Personnel Security*
This should describe all day-to-day personnel security activities including who should have access to the system at all times.

F. *Physical Security*
This should describe all physical barriers to access in the system, drawings, diagrams, and schematics of the system. In addition, risk analysis and audit review information should be included in this portion of the study.

G. *Contingency Plans*
These plans should detail how the critical system functions will be performed if the system is not available. This should include full contingency plan / procedures, post- disaster recovery, and risk analysis.

Teaching Considerations

A. SUGGESTED SCHEDULE

It should be recognized that this module is intended to be a brief treatment of a complex subject within another course. Time will be limited and presentations must be well thought out and effectively presented.

Following is a suggested schedule for time spent on each area:

I.	**Overview**	**0.5 hours**
II.	**System Sensitivity**	**1.0-1.5 hours**
III.	**Security Requirements**	**2.0-3.0 hours**
IV.	**Levels of Security**	**1.0-1.5 hours**
V.	**Data Life Cycle**	**1.0-1.5 hours**
TOTAL		**5.0-8.0 hours**

B. HOMEWORK AND EXERCISES

- Identify the sensitive sections of a personnel system.
- Create an access control list that permits individual, group or unrestricted access to 10 or more applications and/or databases.
- Identify four levels of security and describe the possible differences in the authentication process for each of these levels.
- Review the life cycle of data and information in an organization. Write a policy statement for the destruction of 'stale' data.
- Write a statement of company policies for: Access Control, Violations, or Password Management

C. CASE STUDIES

This module lends itself well to the use of case studies. These will clarify the various aspects of system security and lend realism to the subject.

Suggested case studies involve two general areas:

1. Systems that have a single sensitivity level.

   The single level system might be something like an Automatic Teller Machine (ATM) or an Electronic Funds Transfer (EFT). The ATM is characteristic of low value transactions where financial limits are balanced against ease of use. EFT systems; on the other hand, are high value operations where ease of use is sacrificed for the assurance of accurate identification and authentication.

2. Those systems that involve a mixture of different levels.

   In the multi-level security area, a MIS containing a mixture of sensitive and non-sensitive data is a good example. In this system the use of increasingly complex identification and authentication as the sensitivity of data increases can be shown.

Another area that can be addressed is the movement of some systems from a tightly controlled environment to a more open environment where effective, but friendly, access control must be extended to remote users, such as in customer oriented banking.

Bibliography

National Computer Security Center, “A Guide to Understanding AUDIT in Trusted Systems, NCSC-TG-001-87, 1987. 9800 Savage Road, Fort George G. Meade, MD 20755-6000

The guidelines described in this document provide a set of good practices related to the use of auditing in automatic data processing systems used for processing classified and other sensitive data.

U.S. Department of Defense, “Trusted Computer System Evaluation Criteria” DOD 5200-28-STD, December 1985.

Obtain from Office of Standards & Products, National Computer Security Center, Ft. Meade, MD 20755-6000, Attn.: Chief Computer Security Standards.

COMMUNICATIONS SECURITY

Revised August 1990
Revised May 1995
Revised February 2001

National Information Assurance Training and Education Center
College of Business
Idaho State University
Claude Walston
University of Maryland

Description

This module is intended to be included in an undergraduate course on data communications and networking for information systems and business majors. Several perspectives could be chosen as the basis for this module: an example might be, a detailed technical perspective for students who are interested in designing data communication systems and networks.

However, this module is written from a management perspective for those students who want to become intelligent users of such systems or those who aspire to a management role in an organization that relies on data communications systems or networks to interconnect elements of its information processing systems, either internally or externally.

The module is designed to be added to an existing data communications course, or it could be added to a course in office automation. If the institution is using the DPMA Model Curriculum for undergraduate Computer Information Systems, then it could be added to CIS/86-15, (Distributed Intelligence and Communication Systems).

The topics covered in this module are:

1. a review of the concepts of protection in data communication systems and networks;
2. the interrelationship of communications security and network security for interconnected elements, such as PC's, workstations, mini and mainframe computers, Etc.;
3. a description of the threats to data and information assets and resources in communications systems and networks;
4. a description of countermeasures and protection mechanisms to these threats (including encryption);
5. the need for cost/benefit tradeoffs to be made.

COMMUNICATIONS SECURITY

OBJECTIVES:

The objective of this module is to present the advanced concepts of information protection in data communication systems and networks.

LEARNING OBJECTIVES

Upon completion of this module, the student should be able to:

- Explain protection concepts for data communications systems and networks;
- Identify threats to data communications systems and networks and appropriate countermeasures;
- Recognize the need for tradeoff studies of the costs and benefits involved in achieving communications security.

PREREQUISITE:

The student should be a senior and should have completed courses in both computer systems hardware and software. The student should also have taken courses that included the modules Introduction to Information Protection, PC/Workstation Security, Security Fundamentals, Systems Security or similar classes.

Topic Outline:

I. Overview
A. Review Of The Concepts Of Protection In Data Communication Systems And Networks From A Management Perspective.
  1. Systems Objectives: Controlled Sharing Of Information And Resources.
  2. Specific Needs: Privacy, Secrecy, Integrity And Availability.
  3. Policies And Mechanisms.
  4. Assets: Identification Of Valuable/ Sensitive Data And Information.
  5. Threats And Vulnerability.
B. The Interrelationship Of Communications Security And Network Security For Interconnected Elements:
  1. Systems Connectivity
  2. Public/Private Carriers
  3. Relationship To Reliability And Dependability
II. Threats
A. Types Of Attacks/Failures
  1. Passive Intrusion
    a. Disclosure Of Message Contents
    b. Traffic Analysis
    c. Disclosure Of Data On Network Users
  2. Active Intrusion
    a. Modification Or Deletion Of Message Contents
    b. Insertion Of Bogus Messages
    c. Replay Or Reordering Of Messages
    d. Viruses
  3. Natural Disasters/Catastrophes/Sabotage
    a. Human Errors
    b. Fires, Floods, Brown-Outs.
B. Locus Of Attack/Failure
  1. Terminals
  2. Hosts
  3. Front-Ends
  4. Gateways
  5. Links
  6. Switches (Includes Multiplexer, Intermediate Nodes)
  7. Interconnected PC/Workstations (Includes LAB, Host-PC Etc.)
III. Countermeasures
A. Encryption
  1. Private-Key And Public-Key Systems - DES And RSA As Examples
  2. Key Distribution
  3. Link Level And End-To-End
B. Authentication
  1. Node And User Authentication
  2. Passwords

3. Message Authentication
4. Encryption-Based
5. Added Protection For PC Authentication Date

C. Access Control
1. Access Control Mechanisms-Control Lists
   And Passwords
2. Administration

D. Contingency Planning

IV. Tradeoffs-Costs & Benefits

A. Accessibility Versus Secrecy

Annotated Outline

I. OVERVIEW

Connectivity and communications systems are intertwined. The major thrusts of computer development in the past forty years have been the growing ease of use and growing interconnection of systems. Today, major manufacturers market computers that use compatible operating systems, from microcomputers to mainframes (UNIX or DOS). Postscript is a language accepted by an ever-increasing number laser printers and by almost all new typesetting machines; it is becoming a standard language for describing marks on paper. Word processors are available that accept files from IBM compatible machines into Macintosh computers and vice versa. Networks may span continents, or simply connect rooms.

Connectivity means more than compatible operating systems, compatible languages, communications, and in a holistic sense, computers simply become more pervasive and easier to use. Like a telephone network, the utility is used, with the user unaware of details of the pieces such as DOS or satellite protocols in the case of long-distance telephone.

The presentation of this module reviews the basic concepts of protection as it is applied to communications and network security. There is a misconception that this topic applies only to large organizations with externally interconnected systems. However, even managers who do not have computers connected to communication systems but who do use telephone systems (private or public) for business purposes should recognize that they may also have vulnerable attack points. Competitors can do simple traffic analyses of outgoing calls to determine major clients or suppliers, dishonest employees may use the office phones improperly, etc. While the countermeasures may be simple, the principles covered in this module still apply. Furthermore, if small businesses have only two or three interconnected PC's and printers without any external connections, they should also apply network security principles because accidents, such as employee failures or errors can cause major problems, e.g., data loss.

Managers, users and designers of communications systems and networks are faced with a paradox. These systems are designed to facilitate the sharing of information, resources and services by legitimate users but simultaneously they must be protected from unauthorized entry and malicious attacks.

In this section, survey the concepts of policies and mechanisms and their roles in protection. The aspects of assets, threats and vulnerability are also reviewed.

Summers points out that since users increasingly access computing systems from remote locations, careful attention must be given to communications security. Also, security is increasingly important when connecting computers into networks or implementing distributed systems. Because of this, relatedness, consider communication and network security together.

II. THREATS

A variety of threats or failures that threaten communications and network security, can be grouped into three major categories:

- Passive intrusion
- Active intrusion
- Natural/Sabotage

In passive intrusion, messages and message traffic over the network are observed but not modified or disrupted. Passive intrusion focuses on the interception and reading of communications messages being transmitted between elements of the system, on the analysis of message lengths and traffic flow and traffic patterns in the network, and on the identification of network users. Passive intrusion can be accomplished many ways, for example: wire tapping, emissions monitoring and interception, or by posing as a legitimate user. The users and operators of the system are quite often unaware that passive intrusion has happened.

Active intrusion is done with the specific intent of adversely affecting system operation. It includes actions such as erasing or altering messages, reordering messages, generating bogus messages or disrupting service by overloading the network.

Computer viruses are particularly new and dangerous form of active intrusion. These computer programs infiltrate a computer system and attack the operating system, application programs, and data in the same way a cancer virus or retro viruses attack the human system. They can lie dormant for a time, hidden from the user or operator of the system, before they become active. By the time they are discovered, a great deal of damage may have occurred and much data may have been destroyed and lost. Viruses are composed of three parts:

- A mission component (such as to delete files, send data to a certain user, etc.);
- A trigger mechanism (which activates at a specific time or with the occurrence specific event, e.g., the person's name not being on the payroll list); and
- A self-propagating component (whereby it attaches itself to files, programs, or whatever the creator of the virus is in search of).

The threat from viruses increases when interconnected systems are involved because the virus can be injected into one element and quickly spread to other interconnected elements or have access to the infected element.

The third category of threats or failures is the one composed of natural disasters, catastrophes and sabotage. The most significant threat to systems comes from mistakes, both errors and omissions, on the part of users or operators of systems.

Networks and communications systems must support a high degree of interconnectivity as well as a large diversity of elements. They provide a number of locus points vulnerable to attack by an intruder. If the network is not designed properly, failure of some of these points can also jeopardize the operation of the network and result in the loss of service. PC's and workstations provide particularly good targets.

III. COUNTERMEASURES

Many approaches have been developed to counter potential threats to the security of communications systems and networks. These approaches are identified in this section. One countermeasure is encryption, as described in. Encryption systems use a key with their cryptography algorithms to convert plain text ("clear-text") into encrypted text ("cyphertext") or vice versa. There are two approaches to encryption. In the private-key system the same key is used at the transmitting and the receiving channel, and the key is transmitted through a secure channel to both stations. An example of a private key system is the DES (the Data Encryption Standard) of the National Bureau of Standards. The second approach is the public-key approach where separate keys are used at the transmitting and receiving stations, a public procedure for encryption and a private procedure for decryption. RSA is the most promising public key system. Keys have finite lives, so they must be generated, distributed and historical records kept. This presents distribution problems. See for a review of solutions.

Another important tool in providing network security is authentication. This involves verifying that a user who wants to access the system is who he or she claims to be. Passwords are the most commonly used authentication devices. Another form of authentication applies to messages transmitted over the network to insure that they were not changed in transmission and do come from the claimed source. PC's and workstations used in networks present very special authentication problems.

Access control is another important countermeasure to provide network security. This requires identifying the privileges of a user before his accessing information or using the services provided by elements of the network. This control will also operate a process to insure that the user can only access and use what he or she has been granted permission.

Dealing with the threat of natural disasters or catastrophes presents very special challenges. Risk analysis and contingency planning are two tools designed to counter these threats. The module on Corporate Security Management deals with these issues.

The technical and political aspects of the 'Clipper Chip' debate should be discussed fully. This topic will not be going away and is a critical management issue.

V. TRADEOFFS-COSTS AND BENEFITS

The measures taken to achieve communications system security are not free; there are costs implementation involved. The manager of the system has to determine whether the costs associated with the potential loss of assets, services and resources are sufficiently greater than the costs of providing protection and therefore, justify implementation of security measures. Describe and illustrate an organized approach to the cost/benefits study with a good example.

VI. NETWORK DESIGN[1]

In this section, different aspects of secure network design should be covered. The basics concepts of the cryptographic checksum to ensure message integrity and secrecy should be described. The concept of a trusted network should be developed. Of course, it is complicated by two factors:

- the number of components/media/systems involved in a network, and
- the fact that an active subjects interfere with other active subjects on a network.

The possibility of compromise of a node or a communications link is serious because it implies a continuing need for assurance of authenticity of any trusted network base. A paper by Randell and Rushby represents an example of separation of a distributed system into trusted and untrusted components.

1 *Network Security*, Charles Pfleeger, Unpublished Report M-381 (HQ 87-32813/1

Teaching Considerations

A. SUGGESTED SCHEDULE:

The following sample module plan is based on the offering of three to five and a half hours of lectures:

I. Overview.. 0.5 hours
II. Threats .... 1.0 to 2.0 hours
III. Countermeasures .... 1.0 to 2.0 hours
IV. Tradeoffs - Costs and Benefits.................................... 0.5 to 2.0 hour
V. Network Design.. 1.0 to 2.0 hours

B. HOMEWORK AND LAB EXERCISES

A specific lab exercise on protection cannot be justified in this module. It would be more appropriate to incorporate security concepts in the lab exercises used in the general data communications course. Specify the facilities available at a particular location.

C. CASE STUDIES

Two possible forms of case studies are suggested. The first is based around a particular application, such as a remote login or electronic funds transfer. The particular vulnerabilities and countermeasures of that application are studied. The other form of a case study is analysis of the security and vulnerabilities and features of an existing network, such as the ARPAnet.

Bibliography

Summers, R.C., “An Overview of Computer Security,” *IBM Systems Journal*, Vol. 23, No. 4, 1984, pp. 9-25 (also in [Abrams 86]).
A good management overview of the major aspects of computer security.

Courtney, R.W. & Todd, M.A., “Problem Definition: An Essential Prerequisite to the Implementation of Security Measures,” In *Computer Security: a Global Challenge*, Proceedings of the Second IFIP International Conference on Computer Security, IFIP/Sec 84, North Holland, 1984.
A review of the problems solved about computer security.

Denning, D.E., *Cryptography and Data Security*, Addison-Wesley, 1983.
Presently this is one of the principal textbooks in computer security. Good as a background reference.

Voydock, V. and Kent, S., “Security Mechanisms in High-Level Network Protocols,” *ACM Computing Surveys*, Vol. 15, No. 2, June 1983, pp. 135-171.
Threats, cryptographic controls, and use of end-to-end encryption in networks.

Davies, D.W. and Price, W.L., *Security for Computer Networks*, John Wiley and Sons, 1984.
A study of network security, primarily achieved through encryption. Completed description and analysis of DES.

Meyer, C. and Matyes, S.M., *Cryptography A New Dimension in Computer Data Security*, John Wiley & Sons, 1983.

Definition and use of encryption including a full description of link and end-to-end encryption.

Schou, C.D., Fites, P.E., & Burgess, J.D., "Corporate Security Management," in *Information Security Modules*, Department of Defense, 1989.

Consider this the capstone security module in this document. Emphasis is on the management of a corporate level data security program.

CORPORATE SECURITY MANAGEMENT

Corey D. Schou, Ph.D.
National Information Assurance Training and Education Center
College of Business
Idaho State University

Description:

This module deals with top management and policy considerations. Responsibilities of managers vary, depending on their level in an organization, and this module introduces differences in responsibilities at various levels of management. The role of the System Security Officer (in organizations large enough to warrant a SSO) is discussed.

A corporate security management plan needs the involvement of all levels of management to ensure that the program is properly and thoroughly implemented. The program should clearly identify local, state, and federal legislation that defines responsibility to ensure that all members of the corporation understand and are able to implement a specified plan. Ultimately, the corporation is held responsible for the accuracy and integrity of corporate data.

This module is intended to be included as part of a course, such as the CIS/86-18 (Information Resource Planning and Management). Other courses, such as those specialized in security or data processing management concepts, might include this material, at least in outline. A Business Policy course that has a significant MIS component, could benefit from including this module as a case study or as part of examining the responsibilities of senior management to interact with the external environment.

CORPORATE SECURITY MANAGEMENT

OBJECTIVES:

The objective of this module is to introduce students to the basic concepts of managing a corporate level security program, including planning and implementation. All students should know at least a few of the basic methods included here.

LEARNING OBJECTIVES

Upon completion of this module, the student should be able to:

- identify the objectives of developing a corporate security program.
- identify the major components of a corporate security plan.
- identify the responsibilities of different levels of the corporate structure for a corporate security plan.
- discuss the security considerations of computer connectivity and different organizational structures.
- identify the rationale for risk analysis.
- define contingency planning and describe its place in corporate security management.
- list and discuss the legal issues associated with corporate security management.
- define system validation and verification.
- discuss the role of the Information systems audit function and how it fits into corporate security management.

PREREQUISITES

Students should have completed the following classes or their equivalent. Principles of Management, Organizational Behavior, and Introduction to Computer Information Systems. Business Policy would be of benefit either as a pre- or as a co-requisite.

Topic Outline

I. Overview
II. Development of Security Program
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, Corporate structure, and security.
   1. Connectivity defined
   2. Affect on Corporate Structure
   3. Security considerations
D. Plans
   1. Human Resource Management
   2. Access Control
   3. Data Control
   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
III. Risk Analysis
   A. Reason
   B. Typical Contents
   C. Main Purposes
IV. Contingency Planning
   A. Defined

B. Backup
C. Critical Elements
V. Legal Issues for Managers
A. Licenses
B. Fraud/Misuse
C. Privacy
D. Copyright
E. Trade Secrets
F. Employee Agreements
VI. System Validation & Verification (Accreditation)
A. Plan Testing
B. Acceptance of Responsibility
VII. Information Systems Audit
VIII. Computer Security Check List
A. General Information
B. General Security
C. Fire Risk and Water Damage Analysis
D. Air Conditioning Systems
E. Electrical Systems
F. Natural Disasters
G. Backup Systems
H. Access Control
I. System Utilization
J. System Operation
K. Software
L. Hardware
M. File Security
N. Data File Standards
O. Shared Resource Systems Security

Annotated Outline

I. OVERVIEW

Every corporation has a responsibility to itself, to its clientele, and to society in general, to exercise good control over its information systems. Internal operations rely on accurate and timely data and information; personal data about employees and clients must be kept confidential; and much of the corporation's competitive position may depend on controlling the information it has. All these, and other factors, imply that a corporate security plan is an important element in proper operation of a firm.

II. DEVELOPMENT OF SECURITY PROGRAM

A corporation needs a general security policy. The policy must be developed and supported by management at all levels of the organization, from the highest to employees at the operational levels. Critical elements for the development process of a corporate security plan, as for any other planning process, include defining objectives, defining policies in support of those objectives, and devising plans to implement the policies. (Senior management and board of directors are responsible for defining objectives and policies rests at the highest level; lower levels of management devise plans and implementation strategies). People at all levels must be aware of their individual responsibilities.

A. *Objectives*

Three activities are recommended as a basis of the general security policy:

- Identify sensitive systems and data;
- Create plans for ensuring security and control of such systems;
- Develop and implement personnel training programs.

The most compelling argument in support of security management from the corporation's standpoint is that confidential data may give a competitive advantage. The firm may lose this advantage may be that is lost if controls break down, with the consequent possibility of the firm's demise if legal requirements have been violated materially.

Each corporation has its own strategic imperatives; objectives for a corporate security plan will follow, combined with the guidance offered by applicable legislation.

B. *Policies*

The board of directors and senior management of a corporation must set strategic objectives for the management of corporate security; policies to guide implementation are also a senior level responsibility. Specific examples of policies change from company to company, but most include statements like, "This firm is committed to ethical and professional behavior." One model for corporate policies is found in the Data Processing Management Association's Model Corporate Security policy; other models are available in various texts including or.

C. *Connectivity, corporate structure, and security.*

1. Connectivity defined

The major thrusts of computer development in the past forty years have been the growing ease of use and growing interconnection of systems. Today, major manufacturers market computers that use compatible operating systems, from microcomputers to mainframes (UNIX or DOS). Postscript is a language accepted by an ever increasing number laser printers and by almost all new typesetting machines; it is becoming a standard language for describing marks on paper. Word processors are available that accept files from IBM compatible machines into Macintosh computers and vice versa. Networks may span continents, or simply connect rooms.

Connectivity means more than compatible operating systems, compatible languages, communications, and in a holistic sense, computers simply become more pervasive and easier to use. Like a telephone network, the utility is used, with the user unaware of details of the pieces such as DOS or satellite protocols in the case of long-distance telephone.

2. Effect on Corporate Structure

Connectivity makes a physically and/or organizationally decentralized form of corporate structure much easier to support. Connecting computers accommodates moving decision making as close as possible to the point where workers actually accomplish things. There are many reasons a decentralized structure may be chosen (see any text on organization structure for examples); connectivity makes it simple.

3. Security considerations

When planning the basic structure of the organization, the board of directors and senior management should be aware that there are security risks involved in moving to greater connectivity. One may purchase a personal computer, write one's own software for everything desired, and never communicate with another system; this computer is almost totally immune to things like computer viruses. Connectivity refers to a system of communications exposures, exposures caused by using programs created in an unsecured environment in a formerly secure environment.

The details of the exposures are covered in other available modules (Database System Security, Communications Security, Systems Security). In the context of corporate security management one must recognize that increased connectivity implies increased exposure.

D. Plans

Plans to implement security policies depend on the level of management involved. Operations management may be concerned with subjects like physical access to a computer room; user department management may be concerned with correct use of application systems; human resources management may be concerned with proper training programs and career path counseling, and so on. Items which must be included in any effective set of security plans include:

- Access Controls: identify and authenticate users to protect against computer crime;
- Data Security Programs: base data security programs on the fact that a corporation depends on its computer system.
- Data Labeling: safeguarding sensitive data to the degree of control necessary for defined protection.
- Human Resources Planning: hire properly qualified people and ensure good employee—management relations and effective training programs.
- Contingency Plan: plan for problem avoidance and recovery.
- Legal Responsibilities: understand and provide for legal requirements.

More material about the elements of these plans is available in several references.

E. *Responsibilities*

Board of Directors and Senior Management define corporate security objectives;

Senior Management and Board of Directors define corporate security objectives, define policies to achieve these objectives, and ensure that mechanisms for communicating those policies are in place. This may include tying both compensation and promotion of managers to success in meeting the corporate security objectives.

Middle Management (e.g., Human Resources Manager, DP Manager, Plant Management) defines staff procedures to ensure proper policy implementation;

Employees are responsible for ensuring that elements under their control are carried out according to policy and procedures to maintain effective control and security.

III. RISK ANALYSIS

Begin the actual development of a plan with some form of risk analysis. At the least, identify sensitive systems and data; the estimate the value of these systems; and identify threats, such as listed below. If developers do nor assess the risks faced and the value of assets exposed, the security plan really is in a vacuum and cannot be very effective.

Many kinds of risks can be identified; these vary depending upon the situation, but typical ones include:

- Sabotage (Trojan horse, trap door, time bomb, virus, worm);
- Environmental(fire, flood, power outage, etc.) ; and
- Errors (input entry mistakes, poor quality control in system development, etc.)

Many methods have been developed to quantify risk analysis data, the purpose of which is to reduce inexact opinions to a form that permits adding up exposures and determining a dollar figure. Various metrics, including so-called “fuzzy metrics,” may be used.

Formal methods include estimating the probability of loss, multiplying by the value of the exposed asset, and adding these numbers (see, for example). In practice, this approach tends to lead to a sea of numbers that loses all real meaning (“paralysis by analysis”). The ease with which computers produce numbers has not helped this simplify problem.

Two main purposes of risk analysis are to:

- Assure that management does not overlook significant intentional or accidental threat to the information system;
- Assure that by cost-benefit analysis, management avoids spending more to control an exposure than the potential loss.

IV. CONTINGENCY PLANNING

The key elements of a contingency plan are “protection, detection, and recoverability.”

A contingency plan acknowledges that disaster can happen: the organization must design a plan to accommodate the survival of organizational operations in the event of flood, fire, earthquake, electrical disturbance, or other unexpected events that can disrupt the organization’s systems. Risk analysis should offer guidance on the likelihood of various contingencies, and in what resources to invest providing such recovery methods as off-site systems, backups and so on. Several references discuss contingency planning.

Every effective contingency plan must consider backing up data files.

Most critical to the firm is that a contingency plan:

- exists;
- is communicated to employees; and
- is tested regularly.

V. LEGAL ISSUES FOR MANAGERS

Managers, particularly senior managers, must deal with potential legal problems and requirements (the most complete treatment for the non-lawyer is in) These include:

A. *Licenses*
Application software for microcomputers, and even for large installations, normally is licensed rather than owned. The organization risks serious legal problems if terms of the license are not followed

B. *Fraud/Misuse*
Fraud is straightforward -- corporate security planning must include consideration for possible fraud by employees, contractors, customers, or non-associated people. Misuse includes penetration by unauthorized users, unauthorized copying, negligence and similar exposures.

C. *Privacy*
The organization may have legal, or other responsibilities to safeguard data about customers, employees, or others from disclosure.

D. *Copyright*
Related to licensing, some organizations may need to be very careful about copyright. Publishers and educational institutions are obvious candidates here.

E. *Trade Secrets*
Trade secret legislation is one method open to organizations to protect their confidential data. The corporate security plan should identify circumstances, if any, where trade secret may be appropriate. Use of trade secrets to protect confidentiality imposes certain, legal requirements on the organization, and the overall plan should identify these requirements.

F. *Employee Agreements*
Among the issues involved in protecting trade secrets is the need to ensure that employees are aware that they are secrets. This usually is accomplished through an employment contract (plus other administrative actions of the organization's operations.) A typical contract includes clauses limiting employee use or disclosure of corporate data after the employee leaves. The corporate security plan needs to address clauses needed in employee contracts.

VI. SYSTEM VALIDATION & VERIFICATION (ACCREDITATION)

Test contingency plans; similarly, it is critical to test all aspects of the corporate security plan. Does the plan meet the originally identified needs; does it work as planned? Accreditation occurs when a responsible manager "signs off," that is, attests that the system is in conformance with the plan. The appropriate signing authority depends on the portion of the plan in question.

VII. INFORMATION SYSTEMS AUDIT

The information systems' audit employs an outside entity to assess the organization's corporate security (and other information systems) plan. The auditor should attest whether or not the plan meets accepted standards, and should identify strengths and weaknesses.

VIII. COMPUTER SECURITY CHECK LIST

Since this module represents the capstone effort of the computer security curriculum, include a checklist for computer security. Necessarily, aim this list at large organizations with mainframes; the list also includes most information needed for microcomputer system security.

A. *General Information*

1. A detailed Statement of Threat for the organization.
2. A Statement of Threat for individual locations.
3. A list containing phone numbers for all individuals involved in the organizational security.
4. A policy document detailing how the security personnel have access to the MIS personnel.
5. Documentation on the training of all MIS personnel.
6. An organization chart and documentation demonstrating the separation of duties to minimize opportunity for collusion.
7. Documentation of a MIS Security Group (MSG) or equivalent. This documentation should include but not necessarily be limited to:
    a. Names, functions, and phone numbers of all members (for emergency access).
    b. Security Specialists, Operations Specialists, Physical Security Specialists, Auditor, Facilities Engineer, Communications Security Specialists, and others with appropriate skills are fully represented on the committee.
8. Documentation for each area that demonstrates that an effective liaison has been established with local support activities in the following areas:
    a. Plant engineering and facilities, construction, electrical, air conditioning, and site preparation.
    b. Physical security.
    c. Personnel.
    d. Safety (Safety Officer, Fire Marshal, Transportation).
    e. Records management.

B. *General Security*

1. Documentation that each area has been designated a restricted area in accordance with current company policy, if appropriate.
2. Documentation of security policies and procedures.
3. Documentation of internal audit efforts that determine compliance with security procedures.
4. Documentation of a formal risk management program.

C. *Fire Risk and Water Damage Analysis*

1. Specific site documentation for fire risk and exposure should contain, but not necessarily be limited, to the following:
    a. The construction techniques that demonstrate the fire resistance of the building containing the system. Raised floors and ceilings, curtains, rugs, furniture, and drapes should be from non combustible materials.
    b. The procedures used to manage the paper and other combustible supplies for the computer facilities. In addition, this should document the control of inflammable or dangerous activities in areas surrounding the computer room.
    c. The storage of magnetic media outside the computer room.
    d. The periodic training of operators in fire fighting techniques and assigned responsibilities in case of fire.
2. Documentation that each site has computer fire protection.
    a. Automated carbon dioxide. If so, do all personnel have training in the use of gas masks and other safety devices.
    b. Halogenated agents.
    c. Water (either wet pipe or preaction alarm).
3. Documentation that portable fire extinguishers are spread strategically around the area with markers visible above computer equipment.
4. Documentation that power shutdown switches are accessible at points of exit. Switches should shut down the air conditioning flow as well.
5. Documentation on the location of smoke detectors. Are they located in the ceiling, under raised floor, in air return ducts? It should answer the following questions:
    a. Will air conditioning systems shutdown on detection of smoke?
    b. Who will perform the engineering analysis of function of smoke alarms and how often?
    c. Who tests smoke detection system and how often?
    d. Who is responsible for fire drills and how often should they occur?
6. Documentation of sub floor cleaning and contents, if appropriate. It should include:
    a. water supplies for fire fighting
    b. battery powered emergency / evacuation lighting
    c. manual alarm systems
7. Documentation of fire alarm systems to include where they ring, who will respond and how.
8. Documentation of 24 hour attendance and procedures for reporting problems.
9. Documentation of control of potential water damage that includes:
    a. The elimination of overhead water and steam pipes except for sprinklers.
    b. The existence of subfloor drainage including drainage away from all hardware.
    c. The protection of electrical system from water damage in subfloor area.
    d. The water integrity of doors, windows and roof.
    e. The location of sheeting materials for protection of hardware components from water damage.

D. *Air Conditioning Systems*

1. Documentation of the air conditioning system should include:
   a. Unique use of computer air-conditioning system.
   b. The existence of fireproof ducts and filters.
   c. Location of compressor.
   d. Backup air-conditioning availability.
   e. Fire protection of cooling tower if applicable.
   f. Air intake protection with protective screening, and is it above street level.
   g. That the air intakes prevent the uptake of pollutants or debris.
2. Document the temperature and humidity recording and control.

E. *Electrical System*

The electrical system is frequently a weak link in information security. PC/workstations are often overlooked as a source of problems.

Document electrical system reliability by showing:

- That uninterruptible power supplies are available at those locations that require them.
- That motor generator systems are backed up and that there are lightning arrestors on appropriate circuits.
- The reliability of the commercial power supply and that it is clean power if the system relies on it.
- That the security system will continue to function even after a power failure.
- The backup system test frequency and results.

F. *Natural Disasters*

Document the resistance to natural disaster by showing:

- The structural soundness and resistance to windstorms, floods and earthquakes. This would include demonstrating that the buildings are remote from earthquake faults or earthquake proof. Show relationship to geothermal/volcanic areas.
- Proper grounding of all electrical equipment for lightning protection.

G. *Backup Systems*

1. Document the existence of backup systems for all critical systems at the site. This should include, but not be limited to:
   a. A fully articulated agreements for backup computers in -
      1) the same room.
      2) another room in the same building.
      3) a separate location.
   b. Benchmarks or other indicators that the backup systems can, in fact, handle the intended workload.
   c. Copies of the contract granting access to computers owned by others.
   d. Quarterly tests, performed to familiarize staff with procedures for using backup system.
   e. A full security review and plan for backup system ,if needed.
2. Document a full written contingency plan covering:
   a. Individuals who are responsible for each functional area.

   b. A current “who calls whom” list with alternates. This list should include but not be limited to: Management, Emergency Crews, Selected Users, Service Personnel, Facilities Personnel, and Points of contact at backup sites.
   c. Detailed descriptions of the criteria for determining the duration of disruptions to service.
   d. Individual responsibilities for retaining source documents and/or data files for each application.
   e. Individual responsibilities for the destruction or safeguarding of classified materials in the computer facility in the event the facility must be evacuated.
   f. Individual responsibility for the purchase or lease of new or temporary computer equipment.
   g. Individual responsibility for the acquisition of:
      1) Air conditioning equipment.
      2) Computer time/services.
      3) Additional manpower.
      4) Furnishings, cabinets, etc.
      5) Replacement tapes and disk packs.
      6) Alternate sites and their preparation.
      7) Travel accommodations for essential personnel.
      8) Orderly transportation of computer jobs, personnel, and related materials and appropriate coordination with security.
      9) Duplication of backup files.
      10) Continuing security in the contingency mode.
   h. Document the existence of a contingency training program for all computer personnel

H. Access Control

1. Document the access control that is unique to the computer facilities by showing:
   a. That a general guard schedule provide adequate physical security in accordance with the Statement of Threat and a positive identification system exists for all employees.
   b. That the access to computer areas is restricted to selected personnel this would include, but not be limited to:
      1) Unescorted access to the equipment.
      2) Files are segregated so that only specific individuals have access.
   c. That an adequate visitor control procedure exists that including:
      1) Escorts procedures
      2) Proper training of potential escorts about their responsibilities.
      3) Personnel trained to challenge improperly identified individuals.
   d. That security and operations personnel are briefed on how to react to civil disturbances.
   e. That a good liaison program exists with local law enforcement agencies and that suitable articulation agreements are in place.
   f. That all personnel know how to handle telephone bomb threats.
2. Document that background checks and rechecks are performed on all employees.
3. Document that policies exist to ensure that computer employees are cross-trained to cover all essential functions.

4. Document the existence of a continuing personnel education program in computer security matters. This should include but not be limited to:
   a. Knowledge of the provisions of company security policies and procedures
   b. Personnel training of supervisors in human behavior to aid managers in identifying changes in personality and living habits of their people
   c. Personnel training of supervisors so that they can identify possibly disgruntled employees.
   d. Personnel policies that allow for containment or immediate dismissal of employees who may constitute a threat to installation.
5. Document that all exterior windows accessible from the ground level are covered with metal grills.
6. Document that no one can gain access to the computer area without the knowledge of a guard or another employee.
7. Document that the computer facilities are manned by at least two appropriately cleared personnel at all times.
8. Document that housekeeping standards for the computer room includes the prevention of accumulation of trash in the computer area and that floors (and associated under floor areas), equipment covers and work surfaces are cleaned regularly.
9. Document that waste baskets in the computer room are of metal material with closing tops and that they are dumped outside the computer area to minimize dust.
10. Document smoking rules in the computer facility. If smoking is allowed, document the existence of self-extinguishing ash trays.

I. System Utilization

1. Document that the hardware utilization policy includes but is not limited to:
   a. that systems comply with operations schedules
   b. that techniques exist for matching meter hours to operational hours. This is to ensure that the equipment is not being used for unauthorized purposes during off duty hours.
   c. that a regular maintenance schedule exists for hardware to ensure reliability and that maintenance personnel have appropriate security clearance.
   d. that batch type jobs are logged and cross-checked against an authorized job list.
   e. spot checks of output for possible misuse of a system and that output distribution systems prevent an unauthorized person from receiving a confidential report.
2. Document communications control techniques.
3. Document the existence of emanation security (no RFI detectable outside computer facility).

J. System Operation

1. Document that erasure and declassification procedures include the erasure and overwriting of classified data before the contents of that memory can be reused.
2. Document that the necessary programs, equipment, and procedures exist for declassifying any and all computer equipment used for the processing or storage of classified data on site.

3. Document that policies exist for magnetic tapes and disks that require:
    a. Accountability for use and cleaning frequency of tapes and disks.
    b. Use by authorized individuals only.
    c. The orderly filing of tapes and disks.
    d. Tapes Storage (vertically and in containers) except when in use.
    e. Tape and disk pack utilization records.
    f. The frequent cleaning of tape heads to insure data reliability.
    g. Location of the media library in an area secure from explosion or other dangers.
    h. The use of magnetic detection equipment to preclude the presence of a magnetic field near the magnetic media.
    i. Adequate protection for magnetic media while in transit between locations.
4. Document that media or devices are marked with:
    a. Date of creation.
    b. Highest classification level of any information contained on the media.
    c. Downgrading or exemption instructions when placed in permanent files.
    d. A unique identifier.
    e. The classification of the system's environment when the product was produced, if the assigned classification cannot be immediately verified by the customer.
    f. Special access restrictions.
    g. Color codes.

K. Software

1. Document that software security policy includes the following:
    a. That physical security includes backup file systems at a secondary location for both the programs and the associated documentation. Essential programs, software systems, and associated documentation of programs in the library are located in a locked vault or a secured area.
    b. That access to the essential programs an software systems is restricted to a need to know basis in the prime and backup areas.
    c. That a multilevel access control to the data files (read/write/update, block, record, field, and characters) is provided by various levels of security classification.
    d. That periodic checks are made to validate the security software utilities and the tables of access codes.
    e. That techniques are employed that preclude more than one user updating files at any given time, in those areas where remote access to on-line data bases is allowed.
2. Document that in those areas that allow access by remote terminals:
    a. That keyword or password protection with periodic changes of passwords is employed.
    b. That data is encryption (either hardware or software) techniques are employed during transmission of vital data.
    c. That terminal users are restricted to higher level language access only.

L. *Hardware*

1. Document that the operating systems are protected from unauthorized activity by:
   a. Maintaining built in protection to prevent the bypassing of security utilities and unauthorized access to data bases by a knowledgeable programmer familiar with the system.
   b. Demonstrating that memory bounds are tested following maintenance, initial program load and each restart.
   c. Verifying vendor modifications to the operating system before being installed on the system.
   d. Verifying all local modifications to the operating system by the security officer or personnel designated by him.
   e. Maintaining a record of all operating system modifications until at least the next software release.
   f. Monitoring software technologists to ensure that they do not circumvent the normal access procedures by the use of special coding.
2. Documenting that applications programs are designed to restart using internal recovery procedures.
3. Documenting that all programming changes and maintenance are well controlled. Configuration Control.
4. Documenting that threat monitoring is accomplished by showing:
   a. That a log of those who access data banks or sensitive files is maintained.
   b. That there are software security routines that monitor unauthorized attempts to access portions of the system via on-line notification of an operator or end of day printout.
   c. That attempts to misuse the system are followed up in a systematic manner and according to the appropriate rules established by the SSO and the MIS manager.
5. Documenting that in house service personnel are controlled in their access to vital areas. All non cleared individuals should have special escorts while performing their tasks.
6. Document that a list of vendor authorized service and system support personnel is maintained. That positive identification of these individuals is required and that they do not compromise security.

M. *File Security*

1. Document that on line and off line program files are:
   a. Protected by copies being maintained in a separate building from the original.
   b. Stored in low fire hazard containers.
   c. That there is a current inventory of the files.
2. Document that system backup dry runs are attempted on a regular (quarterly) basis and that the backups contain programs currently under development..
3. Document that program changes are controlled and recorded and that changes are made only to a reproduced version of the original program file with the original left intact.
4. Document that computer operations staff review systems documentation on a regular basis to ensure compliance with operational standards.

5. Document that minimum documentation standards are met throughout all operational sections. Documentation should include but not be limited to:
   a. Detailed production specifications.
   b. A comprehensive narrative description of the function of the program.
   c. Detailed logic or flowcharts following established industry standards.
   d. Current program listings.
   e. Input and output formats.
   f. Output samples.
   g. User documentation.
   h. Copies of test data used to generate output samples following the procedures in the user documentation.
   i. Explanations of codes, tables, calculations and other details unique to the particular program.
   j. Explanations of all error messages, and program halts.
   k. Procedures for handling rejected records.
   l. File sequence descriptions.
   m. Control and balancing instructions.
6. Document that duplicates of all documentation are stored in low fire hazard storage equipment in a separate building from the original.
7. Document that the documentation is inventoried at least annually and that the backups are reviewed periodically to ensure that the documentation package is current.
8. Document that changes in programs and documentation coordinated and approved by the cognizant areas and that theses changes are reviewed by the internal auditor.

N. Data File Standards

1. Document that there is a retention cycle for all data files for all applications. This retention cycle review should include:
   a. Certification that the data and documentation retention cycles are coordinated with the file reconstruction procedures.
   b. Review by the user for compliance.
   c. Certification that the data files are maintained within and under the control of the computer complex rather than the user.
   d. Certification that all files are properly classified in terms of degree of sensitivity and value to the organization.
2. Document that the data files are kept in:
   a. an area other than the computer room.
   b. a fire protected area.
   c. Kept in an access controlled area.
   d. low fire hazard storage containers.
3. Document that dry runs of the data file security system are performed periodically to ensure compliance with standard procedures.
4. Document that the staff members understand and comply with the legal requirements for file retention and that they understand the relative value of the programs and applications.

5. Document that an overall audit control philosophy relating to computer systems concerned assets exists. This philosophy should include:
   a. Computer usage and production controls.
   b. Control of user input to ensure receipt of all data.
   c. Monitoring of output to meet site established standards.
   d. Error reporting and follow-up procedures.
   e. Control of program changes.
   f. Certification that all program options have been tested.
   g. Certification that program conversions provide similar results and do not disrupt production continuity.
   h. A policy detailing the separation of duties.
   i. Policies for both hardware and software backups.
   j. The auditibility of the system.
   k. A policy of auditor involvement during the development cycle.

O. Shared Resource Systems Security

1. Document that for resource sharing systems, remote terminals are available only to selected individuals. This access may be controlled by one or more of the following:
   a. Locked doors.;
   b. Posted guards;
   c. Other approved restraints.
2. Document that terminals are located such that each user's privacy is ensured.
3. Document the use of passwords and the fact that:
   a. they are tamper proof.
   b. they are linked to individuals and locations.
   c. that they are combined with physical keys.
   d. the ability to change passwords is closely controlled.
4. Document that systems software restricts a given individual to specific data files. This access should control the right to add, delete or modify files.
5. Document that the system maintains accurate records of all activity against each data file and that security override procedures are closely monitored.
6. Document the procedures used to monitor the changes to the operating and security systems.

Teaching Considerations

A. SUGGESTED SCHEDULE

1. **Overview..........0.25 hours**
2. **Development of Security Program..........2 to 3 hours**
3. **Risk Analysis..........0.5 hour**
4. **Contingency Planning..........0.5 to 1 hour**
5. **Legal Issues for Managers..........0.5 to 1 hour**
6. **System Validation & Verification..........0.5 hour**
7. **Information systems audit..........0.5 hour**

B. CASE STUDIES/EXAMPLES

Course Project: Develop a corporate security management plan showing type and environment of corporation.

HOMEWORK AND LAB EXERCISES.

C.

Bibliography

U.S. Congress, "The Security Act of 1987", PL-100-235.
This law describes the policy of the Federal Government regarding computer security. Among other things the law covers the identification of sensitive systems, the development of a security program and plan, and the need for training of all users, developers and operations associated with a system.

"Model Computer Crime Act," Data Processing Management Association, Park Ridge, IL, 1986.
This model act incorporates the establishment of civil procedures for redress of victims of computer crime. The DPMA's model act also proposes forfeiture of property, guidelines for what evidence will be considered in a computer crime case (rules of evidence), a good definition of computer crime, suggested punishments including increased penalties for repeated violations and suggestions for jurisdiction.

Fites, Philip E., Martin P. J. Kratz, and Alan F. Brebner, *Control and Security of Computer Information Systems*, W. H. Freeman/Computer Science Press, September. 1988.
A textbook intended to support college level courses in computer security for technicians and accountants, or to serve as a reference for computer law courses. Contains considerable detail on the material mentioned in this module. A useful reference as well.

Parker, Donn B, *Computer Security Management*, Reston Publishing Company, Inc., Reston, Virginia, 1981.
Another classic, and contains as well considerable information that has not become too dated. One of the primary drivers of the security field has been Donn Parker, and this book covers many topics to which students need exposure in a computer security course.

Pfleeger, A., Network Security, Department of Defense, 9800 - Savage Road, Ft. Meade Maryland, 20755-6000, ATTN: S32.

Module from the Department of Defense 1987 project for computer science/engineering students.

Hsiao, David and Terry Mayfield, *Database System Security,* Department of Defense, 9800 - Savage Road, Ft. Meade Maryland, 20755-6000, ATTN: S32.

A draft curriculum module developed at a workshop sponsored by the National Computer Security Center and hosted by the Institute for Defense Analysis, June 1987.

Walston, Claude, and Lisa Hinman, *Communications Security,*

IDA Memorandum security breach dealing with possible misappropriation of data, computer programs blueprints, plans, laboratory notes or similar material. It is for that reason that the information security specialist will want to be familiar with some basic communications security.

Spiro, Bruce E. & Schou, Corey D., "System Security," in *Information Security Modules,* Department of Defense, 1988.

"Systems Security" is an upper level module that gives a detailed review of security issues and the integration of these details into an organizational security program.

Johnson, Douglas W., *Computer Ethics: A Guide for the New Age*, The Brethren Press, 1984.

This low-cost, readable paperback book introduces critical issues, including: personal data, decision-making and identifying, building and maintaining ethics in a computer society. This book addresses the question of ethics in the indiscriminate use of the personal computer. The concept of what ethics are is proposed and suggestions are made for establishing a code for personal computer use.

Computer Control Guidelines, Second Edition, Canadian Institute of Chartered Accountants (CICA), February, 1986.

One of the most recent publications identifying control points and offering guidelines to auditors and others in the accounting profession.

Lobel, Jr., *Foiling the System Breakers*; Computer Security and Access Control, McGraw Hill, 1986.

This book examines computer fraud and industrial espionage with a focus on access control. It discusses risk analysis, system security policy, selections of tools and technology and the implementation process. One of the best references. There is a mild bias toward Honeywell approaches, but it is limited and mostly confined to specific sections.

Hoffman, Cook & Mayfield, *Risk Analysis*, Department of Defense, 9800 - Savage Road, Ft. Meade Maryland, 20755-6000, ATTN: S32.

Module on Risk Analysis from the Department of Defense 1987 project for computer science/engineering students. Most of the concepts apply equally in the business area, although the quality control material in this module is from an engineer's perspective.

"EDP Threat assessments: Concepts and Planning Guide," RCMP Security Information Publications # 2, Jan. 1982.

Goes into somewhat more detail about one method of attaching dollar values to risks and exposures. Includes forms useful as a guide to setting up this process.

Schmucker, Kurt J., F*uzzy Sets, Natural Language Computations, and Risk Analysis,* Computer Science Press, 1984.

A published monograph that is quite good in explaining what fuzzy sets are, etc. and how to use the concepts in doing asset valuation and risk assessment in security planning. Computer programs for implementing the method are included.

National Technical Information Service, *Risk Analysis Methodology*, AD-A072-249, Dept. of Commerce, Springfield, VA, 1979.

A technical paper describing methods of risk analysis.

Richards, T., Schou, C.D. & Fites, P.E. "Information Systems Security Laws and Legislation," in *Information Security Modules*, Department of Defense, 1989.

Richards, et. al. review topics, timely laws and legislation about computer security as it relates to the individual and the organization.

Gallegos, Frederick, Dana R. (Rick) Richardson, & A. Faye Borthick, *Audit & Control of Information Systems*, South-Western Publishing Company, West. Chicago, Ill., 1987.

This may be the most readable book on the topic. Goes into considerable useful detail about the information systems auditing activity. A useful reference as well. Somewhat technical and probably requires an accounting background to be really useful.

INTRODUCTION TO ACCOUNTING CONTROLS AND EDP AUDITING

Terry L. Campbell, DBA, CPA, CMA, CCA
College of Business Administration
The Pennsylvania State University

Corey D. Schou
College of Business
Idaho State University

Description:
This module is an introduction to accounting controls and auditing concepts intended for a broad variety of students in courses where an appreciation of such concepts is needed. The module outlines key accounting and auditing concepts and describes the various roles played by management, information systems professionals, internal auditors, and external auditors. It deals with management control, application control, evidence gathering and evaluation, and management of the EDP audit function. The module may be used in junior or senior level information systems courses or integrated in other business courses.

Introduction To Accounting Controls And EDP Auditing

OBJECTIVE:

This module is to provide the business and information systems major an opportunity to examine accounting controls and auditing from an overall computer security perspective. These fundamentals give insights into the controls and provide a foundation from which a student may wish to explore these topics in more detail.

LEARNING OBJECTIVES

Upon completion of this module, the student should be able to:

- identify and explain the four goals of accounting controls and auditing: asset safety, data integrity, system effectiveness, and system efficiency;
- explain the roles played by management, IS professionals, internal auditors, and external auditors;
- recognize the control issues in the systems development cycle;
- describe the need for and functions of access controls;
- identify the need for and functions of input controls; 6.describe the need for and functions of communication controls;
- identify the need for and functions of database controls;
- describe the need for and functions of output controls;
- define the approaches used to gather supporting or disconfirming evidence in reference to controls;
- describe the integration of the four goals and the methods by which the evidence may be judged.

PREREQUISITES

Completion of the first two modules Introduction to Information Protection and on Security Fundamentals would be useful. Some Background on management information systems and accounting information systems is desirable. The student should have some computer laboratory experience with shared data, files or electronic mail on a network and/or mainframe.

Topic Outline

Introduction to Accounting Controls and EDP Auditing

I. Overview
A. Role of the accountant
B. Asset Safety
  1. Organizational Asset
  2. Computer Resource Abuses
  3. Value of Systems
    a. Hardware
    b. Software
    c. Personnel
    d. Operating Systems
    e. Application Systems
    f. Data
    g. Facilities
    h. Supplies
  4. Proprietary and Private Data
C. Data Integrity
  1. Pervasiveness of Errors
  2. Individual decisions
D. System Effectiveness
  1. Decision Making Value
  2. Timeliness
  3. Support for Competitive Advantage

E. System Efficiency
   1. Proper Uses of Systems and Components
   2. Misallocation of Resources
      a. Theft
      b. Destruction
         1) Physical Acts of Nature
         2) Physical Acts of Persons
      c. Disruption of Service
         1) Hardware
         2) Software
         3) Personnel
      d. Unauthorized Changes

II. ROLES

A. Management
   1. Top management
   2. Middle Management
   3. Entry-level Management

B. Information Systems Professionals
   1. MIS Orientation
   2. Data Processing Orientation

C. Internal Auditors

D. External Auditors

E. Management Controls

III. SYSTEMS CYCLE

A. Auditor's Involvement
   1. Concurrent Participation
   2. Ex Post Review
   3. Phases and Concerns

B. Alternative Models
   1. Traditional
   2. Prototyping
   3. Socio-technical

C. Differences in Internal and External Auditors'

D. End-user Developed Systems

IV. GENERAL INTERNAL CONTROLS

A. Segregation of Duties

B. Proper Delegation of Authority

C. Competent Personnel

D. Authorization System

E. Documentation

F. Physical Controls

G. Supervision

H. Accountability

V. ACCESS CONTROLS

A. Strengths and Weakness

B. Encryption

C. Personalized Access
   1. Cards and PINS
   2. Physical Identifiers

D. Audit Trails
   1. Accounting
      a. User Identities
      b. Validation Routines Used
      c. Access And Usage Desired
      d. Physical Location Of Originating Site
      e. Session Times And Dates
      f. Access Methods And Number Of Tries
      g. Results Of Access: Authorized Or Rejected
   2. Operations

VI. INPUT CONTROLS

A. Data
   1. Preparation
      a. Conversion to Machine-Readable
      b. Prepare Totals
      c. Human Scanning as Quality Control
      d. Verification
   2. Gathering
      a. Paper-Based
      b. Machine-Based
      c. Mixture
   3. Review
      a. Components
      b. Design
         1) What Data To Gather,
         2) How To Gather Data,
         3) Who Will Gather The Data,
         4) When Will The Data Be Gathered,
         5) Data Handled, Retained, And Used
   4. Controls
      a. Hash Totals
      b. Financial
      c. Document Counts

B. Validation
   1. On-line
   2. Batch
   3. Lexical
   4. Semantic
   5. Syntactic
   6. Corrections

C. Error Controls
   1. Error Report
   2. Field Checks
   3. Record Checks
   4. Batch Checks
   5. File Checks

VII. COMMUNICATION CONTROLS

A. Risks
   1. Reliability
   2. Unauthorized Uses and Abuses
   3. Errors

B. Technical Failure
   1. Communications
   2. Hardware
   3. Software
   4. Personnel

C. Terrorism and Other Overt Threats
   1. Aggressive
      a. Insertion
      b. Deletion
      c. Modification
      d. Intervention
   2. Non-intrusive

- a. Note or File Sending
- b. Monitoring Activities

3. Controls
   - a. Audit Trail
   - b. Operations Audit Trail

VIII. PROCESSING CONTROLS

A. CPU Controls
1. Instruction Set Check
2. Status Check
   - a. Kernel
   - b. Supervisor
   - c. Problem

B. Memory Controls
1. Physical
2. Access
3. Virtual

C. Systems
1. Operating
   - a. Protected from Users
   - b. Insulated from its Environment
   - c. Users Isolated from Each Other
   - d. Examples
2. Application
   - a. Validation Reviews
   - b. Programming Reviews
   - c. Interfaces among Programs/Routines
3. Audit Controls

IX. DATABASE CONTROLS

A. Access to Levels
1. Name
2. Content
3. Context
4. History

B. Application Oversight
1. Update Policy
2. Reporting Procedures

C. Concurrency
1. Replication
2. Partitioning
3. Priorities

D. Encryption
1. Transportability
2. Personalized
3. Multiple levels of Access

E. Physical Security
1. Access
2. File Protection
3. Data Base Administrator (DBA)
4. Backup

F. Audit Controls

X. OUTPUT CONTROLS

A. Production
1. On-line
2. Off-line
3. Ad Hoc

B. Distribution
1. Physical Requirements
2. Control

C. Presentation
1. Content
2. Physical Form
3. Format
4. Layout
5. Time Aspects

D. Interpretation
1. Availability
2. Warning System for Further Information

XI. EVIDENCE

A. Needs
1. Assess Quality of Data
2. Evaluate Processes
3. Review Existence of Processes and Data
4. Initial Review
   - a. Analytical Review
   - b. Statistical Analysis
   - c. Spreadsheet
   - d. Expert Systems / Decision Support Systems

B. Limitations
1. Often After the Fact
2. Constrained To Extent Of Generalized Audit Software (GAS)

C. Generalized Audit Software
1. Parallel Simulation
2. Integrated Test Facility
3. File and Record Extraction

D. Specialized Audit Software
1. Industry Specific
2. Configuration Specific
3. Potential to be More Efficient
4. Less Flexible Than GAS

E. Concurrent Techniques
1. Concurrent Integrated Test Facility
2. Simulations
   - a. Continuous
   - b. Intermittent
3. System Control Audit Review File (SCARF)

F. Human Techniques
1. Interviews
   - a. Preparation
   - b. Observation
   - c. Evaluation
2. Questionnaires
   - a. Determine Objectives
   - b. Plan Questions
   - c. Test
   - d. Deliver
   - e. Analyze
3. Observation
   - a. Work As Participant
   - b. Unobtrusive

G. Flowcharts
1. Document

2. Data Flow
3. Systems
4. Programs

H. Machine Techniques
1. Hardware Monitors
   a. Tracks Activity
   b. Analyzes Activity
2. Software Monitors
   a. Internal to System
   b. Particular Transaction versus Sampling
   c. Analyzes Activity

XII. INTEGRATION

A. Asset Safety
1. Measurement
   a. Qualitative
      1) Questionnaires
      2) Risk Matrix
   b. Quantitative
      1) Expected Loss versus Cost of Controls
      2) Expected Time Loss
2. Cost-Benefit

B. Data Integrity
1. Measurement
   a. Qualitative
   b. Quantitative
2. Cost-Benefit

C. System Effectiveness
1. Objectives
   a. Goals of Firm
   b. Usage
   c. Types of Usage
   d. User Satisfaction
   e. Technical
      1) Hardware
      2) Software
      3) Independence of System Components
      2. Judgment
3. Overall Evaluation

D. System Efficiency
1. Objectives
2. Indicators
   a. Workload Monitors
   b. Systems Checks
3. Overall Evaluation

E. Summary
1. Qualitative
   a. Collect All Items
   b. Think
2. Quantitative
   a. Financial or Business Terms
   b. Sensitivity to Assumptions
3. Judgment
   a. Group Decision Making
   b. Experience Transfer

Annotated Outline

I. OVERVIEW

A. Role of the accountant

The accountant/auditor has a number of roles to play in data processing/information systems environments. These roles include, but are not limited to, asset safety, data integrity, system effectiveness, and system efficiency.

B. Asset Safety

Information as an asset of the organization has long been recognized by management and in general by society. Individuals and organizations accomplish goals by disseminating or withholding information. Safeguarding such an asset is increasingly paramount in the mind set of management.

1. Organizational Asset

As an organizational asset, information and its associated elements occupies a significant share of management's time and effort. The raw accounting numbers cannot reveal the magnitude of importance of the information asset. Consider the cost of market research information, does the cost represent the asset value to an organization that wishes to target a market segment? What about a report on the competition and their likely decisions? What about the cost of a production report? A cash flow analysis? There is a substantial amount of literature that suggests that information is a competitive weapon and that information changes (controls) how a firm might compete, manage, govern, and survive.

2. Computer Resource Abuses

Unfortunately, computer resource abuses occur, even in the best of organizations. The key thing to note is that the most common abuses seem to be in information omissions or errors. These errors cause losses to the organization through ineffective and inefficient decision making. Physical catastrophes are the next most common category. These catastrophes include fire, hurricane, flood, power interruptions, and other physical disasters. A substantial set of preventative and recovery measures exist for these disasters. Finally, there is the abuse with the more visible press clippings: fraud, embezzlement, and other unlawful uses of the system.

Though one of the latter abuses may be the theft of computer time, it seems unlikely that this is a major contributor in the abuse category. Rather, electronic funds transfer, that permits the amounts to be substantially larger than in a manually executed fraud or embezzlement, appears to be of more primary concern.

Individual state laws are being updated and/or have been updated to recognize and take action or correction in the current state of technology including fraud and embezzlement. Accountants and auditors are concerned with safeguarding assets and the proprietary nature of the information contained in the system. Their concern about unauthorized access to information for which there is no valid business reason to provide system access to a particular user or inquirer directs a 'need to know' rule. Other functional managers will recognize the same as their information leaks to competitors or helps to get a business started by a former employee.

3. Value of Systems

One cannot deny that systems have value. One may have difficulty stating the value in terms that are understandable and acceptable by the various stakeholders. An accountant/auditor is confronted with the difficulty of accurately assessing the value of each system components; however, the initial outlay of each component is more easily measured than the value of the system. The accountant/auditor might need to acquaint management with the risks of system disruptions in order to focus attention on the value of the systems.

a. *Hardware*

Hardware costs are decreasing per unit of CPU time, storage capacity, memory; and making the acquisition of ever increasing powerful computers a normal occurrence. Thus, hardware acquisition becomes an important variable for management review. In addition, networks and workstations are moving more power to each desk. Accountants/auditors need to be alert to appropriate cost-benefit analyses and security issues relative to desktop computing.

b. *Software*

Software costs must be managed regardless of the source of the software: custom or package. Software evaluations become critical as the organization tries to develop common applications across the organization. Accountants/ auditors must monitor the evaluation and selection of common software to minimize the capital investment as well as the training and integration costs.

c. *Personnel*

Adequately trained personnel are an asset to the organization, yet, no accounting treatment exists for the recording of such assets. Special attention should be paid to information systems professionals relative to stress and possible burnout and the resulting negative results. Special skills are at a premium and the organization may have to increase reliance on third-party vendors to provide these special skills.

d. *Operating Systems*

Operating systems are composed of the set of programs that tell the computer how to 'operate' the computer and the application programs. There is increasing need to monitor these operating systems in order to optimize the performance of the system. In addition, the operating system needs to be carefully controlled to prevent intrusion or misuse.

e. *Application Systems*

Application systems are the programs that actually direct the computer to perform calculations and other activities directed towards the desired end results. Maintenance of these programs, whether purchased or in-house developed, becomes a central theme of the accountant/auditor as these systems are often modified with or without appropriate review and oversight. The modification routine is a key internal control function.

f. *Data*

The organization's data are its lifeblood. The operating and application systems are nothing without data. The data are converted into information to provide reports, etc. to management for decision making. Thus, the integrity of data becomes paramount as an organization strives for competitive advantage. Even before competitive advantage, the organization must rely on timely and accurate data for its daily routine operations.

g. *Facilities*

The physical facilities necessary to provide a secure location for the hardware, software, and personnel comprise a significant asset for the organization. One key thing to evaluate is the extent to which the facilities have been reviewed and evaluated for security of hardware, software, and data, and up-to-date cost effectiveness. Local facilities are important as well as back-up sites. These back-up sites, identified in the disaster recovery or contingency plan, may be either hot or cold; a hot site is one with computers and systems available and cold site is one with a minimal time delay necessary reestablish operations.

h. *Supplies*

Numerous supplies are necessary just to operate the systems. These supplies include tapes, disks, etc.; many of which need to monitored, not because of the intrinsic value but rather as a general part of controls. In addition, the amounts of data to be damaged, stolen, destroyed, or misclassified without authorization behooves management to exert control over these assets, too.

4. Proprietary and Private Data

With the availability of mass storage and increasingly large databases, the possibility of abuses becomes greater. The converse of this argument is that the data is increasingly valuable to the organization for competitive purposes. The accountant/auditor evaluates the extent to which these valuable data are protected and used properly.

C. *Data Integrity*

Data integrity means the extent to which the data item represents the 'truth' expected. Thus, data must have aspects such as completeness, representativeness, stability, truthfulness, timeliness, and be uncontaminated. These aspects are gained only at a cost; cost benefit analysis must be used to assess the procedures and controls necessary to maintain and protect data. Unfortunately, the value of data is not easily calculated. Accountant/auditors work with management to assess the cost of controls and the willingness to implement them.

1. Pervasiveness of Errors

Because the system necessitates the sharing of data, an error can permeate the system and cause erroneous decisions to be made. Input controls and edit checks take on added importance as the systems become more integrated.

2. Individual decisions

Even if the information is only used by one decision maker, the need for integrity is still present. A single decision made without data integrity may lead to significant negative results.

D. *System Effectiveness*

The assessment of the degree to which a system (purchased or in-house) meets its objectives is a task often assigned to the accountant/auditor in order to get an objective viewpoint. The system effectiveness check may be done after a project has been in operation for a period of time or done at periodic stages of the design process.

1. **Decision Making Value**
   Management may wish to assess the extent to which the system has provided information for decision makers and the value that was added by having the system. Careful review of the decisions and the information systems permit the accountant/auditor to comment on the system effectiveness.

2. **Timeliness**
   Getting the right information is not sufficient to ensure effectiveness; the system must deliver the information at the right time. Thus, the timing and delays must be evaluated for contributing to the timeliness information delivery.

3. **Support for Competitive Advantage**
   In an increasingly competitive environment, it is vital that each element of the organization contribute to the goals of the organization. Information systems for competitive advantage has been a phrase often uttered but seldom operationalized. Yet, the organization demanding the best of its personnel will task their personnel to be observant and opportunistic for possible competitive advantages through information systems. Accountants/auditors will be asked to assess systems effectiveness in light of these demands.

E. *System Efficiency*

Given the increasing resources consumed by information systems it is no surprise that the evaluation of the resource usage is important. Competition for scarce resources is central to the issues that surround information systems. Simply put, there is not enough of any resource to do all the things asked for, needed, or wanted.

1. **Proper Uses of Systems and Components**
   Operating systems, application systems, personnel, facilities, and data must all fit together and be used properly. This fit is developed during the architectural planning phase of the software engineering process. Careful attention must be paid to the utilization of the capacities of each of the elements including the human resources. Proper assessment of utilization can identify the need for improved efficiencies or the need for investments in capacity. The optimization of the elements of the system becomes a critical point in the review.

2. **Misallocation of Resources**
   Improper use of the information systems resources may take on a variety of facets. The accountant/auditor must evaluate these facets for their risk to the organization and suggest compensating controls to limit the risk.

   a. *Theft*
      Theft of hardware, software, and data become increasingly prevalent as systems become more complex but in smaller and smaller physical size. Theft occurs in a number of different ways: outright theft of software or hardware to use for personal reasons or to sell, competitive information to use in starting a competitive business or to sell to a competitor, or the stealing of computer time to conduct personal business.

   b. *Destruction*
      Recent events have suggested that the possibility of physical destruction is increasingly probable. In addition, as organizations look for ways to downsize, the

possibility of overt acts of destruction by disgruntled employees is also increasingly probable. Unintentional destruction and misuse may occur in the normal course of things.

1) PHYSICAL ACTS OF NATURE

Hurricanes, earthquakes, electrical disturbances, temperature extremes, and other such natural disasters must be evaluated and quantified for their risk to the organization.

2) PHYSICAL ACTS OF PERSONS

Physical acts of persons may be made internally by disgruntled employees or customers. Externally, these acts may be in the form of sabotage or espionage.

c. *Disruption of Service*

Service disruptions may be caused by an errant program or by intrusive program such as a virus. Such disruptions must be planned for and contingency plans devised to minimize such interruptions. Organizations need to assess the extent to which the organization can survive if the information system is disrupted; most organizations acknowledge that the survival time is becoming shorter and may be even be measured in hours rather than days.

1) HARDWARE

Computer hardware is vulnerable to electrical problems, fire, and water. The unfortunate facts are that systems do crash and malfunction in a variety of ways. The carryover effect is that personnel become disenchanted and suffer a reduction in morale that may lead to a decline in attention to controls.

2) SOFTWARE

Operating systems and application systems may fail due to incorrect versions being placed in use or improper documentation of system changes.

3) PERSONNEL

Each of the other failure categories may be contributed to by ineffective and inefficient personnel. Employees with emotional problems or inadequately trained and motivated employees can be as destructive any physical catastrophe.

d. *Unauthorized Changes*

Proper controls over changes to operating and application systems must be monitored. Unauthorized changes invite disaster. Careful attention must be paid to mandating proper authorization for changes to programs such as the use of properly executed program change request forms. Discipline is required to act in a controlled manner in responding to emergencies as certain times seem to need emergency measures but emergencies need to be carefully managed in order to minimize the possibility of unauthorized changes.

II. ROLES

Complex organizations necessitate complex roles for the individuals involved. No organization of any size finds this complexity to be a new thing. What is new is the rate of change inherent in a technologically driven organization.

A. *Management*

Management of all ranks and functions play critical roles in the management and control of information systems.

1. **Top management**

   Top management focuses on the policies and strategies of the organization and ensures that the information systems function is well managed. Their primary focus is the strategic business plan of the organization and its alignment with the functional plans of the organization. One such functional plan is the information systems plan.

2. **Middle Management**

   Functional management in all function including information systems management must play participative roles in the planning, design, development, evaluation, and audit of information systems. These participative roles include the development and implementation of the strategies. In this manner the internal audit staff may be involved in multiple roles.

3. **Entry-level Management**

   Entry-level management is oriented to daily tasks and the implementation of controls on an operational basis. Their orientation may be decision oriented but they must be educated to the necessity of good internal controls.

B. *Information Systems Professionals*

Information systems professionals must be an integral part of the management team and not just a service function of technologists. This is increasingly critical as the systems become more integrated with each other and pervasive to the organization.

1. **MIS Orientation**

   MIS professionals are usually oriented to using information systems for solving business problems. Controls are not the primary focus of their attention; business decision making is.

2. **Data Processing Orientation**

   Data processing professionals concentrate on managing a system for optimal performance and timeliness to provide output. Controls may be perceived as a hindrance to optimizing the systems.

C. *Internal Auditors*

Internal auditors are employees of the organization, and must be quite familiar with the organization and its goals. These auditors should posses in-depth knowledge of the organization’s internal control weaknesses and strengths. Major concerns include the effectiveness and efficiency of a system, and asset safety and data integrity. Management may request a management, or operational, audit so to review the efficacy of the EDP function.

D. *External Auditors*

External auditors attempt to assess how well internal controls are in place and functioning in order to determine the extent to which these controls may be relied upon during a financial audit.

E. *Management Controls*

Ultimately, good management controls are the key to reliable internal controls being in place and functioning. Management controls apply to the overall management functions of each level, and function, of managers. The accountant/auditor evaluate the extent to which planning, organizing, staffing, directing, and controlling contribute or hinder the goals of accounting and control. In each situation, certain attributes become more or less important. These management controls may be preventive, detective, or corrective. Preventive controls remove or minimize the problem; detective controls identify the problem; and corrective controls change the problem to the proper status. Regardless, the controls set in place by management are what determines the success or failure of the system.

III. SYSTEMS CYCLE

The traditional systems life cycle of software development can contain from four to twelve phases, but usually the following five: analysis, design, implementation, operation, and review.

A. *Auditor's Involvement*

An audit contains a series of steps: preliminary review, detailed review of management and application controls, compliance testing, substantive testing, and overall evaluation. To develop software for the EDP function of an audit, the auditor must assess the degree to which the system will be relied upon to perform the audit.

Continual discussion and debate has centered on the degree of involvement the auditor should have in the system development phase. The argument centers around possibly reducing the independence of the auditor.

1. **Concurrent Participation**
   Controls may be built into the system by having the auditor's participation throughout the life cycle. Though the role of the auditor may not be clear, the need for controls for large, complex systems is very clear.

2. **Ex Post Review**
   Auditors may be requested to evaluate the controls after a project is completed or after major phases. Unfortunately, the ex post review may not permit a timely introduction of effective controls.

3. **Phases and Concerns**
   If auditor independence is reduced, the credibility of both internal auditors and external auditors may weaken and perceived objectivity may be lost. Thus, management may not place as much confidence in the auditors' statements.

B. *Software Development Methodologies*

Since all systems and environments are different, there is no single method to design systems.

1. **Traditional**
   The traditional approach is sequential and involves analysis, design, implementation, operations, and review, or similar phases. This method is used in situations where system needs are well-defined. The implementation of such systems involves third-party software as well as in-house developed software.

2. **Prototyping**
   Prototyping involves developing a quick trial system that incorporates the user's needed features and functions in a small-scale system, but that can be expanded to a full-blown

system. The opportunity to integrate controls is reduced; but the user may be more satisfied. This method is not recommended for complex systems.

3. **Socio-technical**
The socio-technical approach involves an external agent (consultant) participating in a direct way to develop the system and to change the way the organization functions. This approach does not concentrate on controls unless conscious effort is made.

C. *Differences in Internal and External Auditors*
Internal auditors concentrate on system effectiveness and efficiency, as well as controls. External auditors focus on controls as a guide to understanding the degree of confidence that may be placed on the controls. External auditors may or may not provide recommendations to management on the effectiveness and efficiency of systems.

D. *End-user Developed Systems*
End-users are developing systems more frequently than ever, due to the availability of user-friendly productivity tools and programs. Controls in these systems are nearly non-existent. Yet, these systems are popular because they bypass the difficulty of getting a system developed via normal channels.

IV. GENERAL INTERNAL CONTROLS

The goals of accounting and auditing can be achieved only if proper management controls are in place and general internal controls have been instituted. General internal controls are an integral part of any system, automated or manual. Automation creates problems and opportunities in each internal control.

A. *Segregation of Duties*
Segregation of duties is a primary internal control intended to minimize fraud and embezzlement by assuring that any one person does not have access to two different control functions. In an automated system these functions may be performed without human intervention, that moves segregation of duties to a different status, namely that of separating the operation of the program from the changing of the program.

B. *Proper Delegation of Authority*
Clearly delineated authority and responsibility is essential to good internal control. Increasing integration of data and systems blurs the line, and end-user developed systems accentuate the difficulty. Proper delegation mandates that individuals be designated the 'person in charge' in order to control the system, as well as to reconfirm that management is ultimately in charge of internal system controls.

C. *Personnel*
Consideration for competent personnel is easily neglected when systems are complex and changing often. High mobility and an orientation to technology may reduce the allegiance of an individual to his/her organization. In addition, highly skilled individuals may wish to 'play games' with the system to see if security may be overcome. Personnel morale, training, and commitment need attention so to increase the probability of secure information systems.

D. *Authorization System*
Management grants two kinds of authorizations: general and specific. General authorization are established policies and procedures. Specific authorizations deal with unique, or

infrequent, decisions. Systems automate these authorization processes. The accountant/auditor must direct attention to the computer system's authorization routines.

E. *Documentation*
Systems must be designed to provide an adequate audit trail. Without the audit trail, control is not present and significant serious control problems appear. Even if fraud or embezzlement attempts are not evident, individuals need not be tempted to violate the system because of an inadequacy of the system.

F. *Physical Controls*
Physical controls issues protection of data, information, analyses, plans, overall memory, and equipment. These elements are essential to a viable organization, and a firm should attempt to disburse them geographically so to reduce loss in the case of disaster or malicious intent.

G. *Supervision*
Direct review of personnel is made more difficult because the system permits remote access and electronic performance of many duties. The accountant/auditor must address the need for compensatory controls. A compensatory control may be to evaluate the extent to which the program code and changes are closely supervise and authorized.

H. *Accountability*
Eventually, management is responsible for the institution and operation of controls and systems. The accountant/auditor must ensure that adequate internal controls fully support management's role of control and direction.

V. ACCESS CONTROLS

Access controls are set to verify that an individual or system has the appropriate authority to gain access to the computer system and at what levels within the system the access may be granted.

A. *Strengths and Weaknesses*
Given the increase of shared data as an organization resource, access controls are vital to the integrity of such resources. At the same time, limited access, or restricted access, may upset users who do not perceive the need for control nearly as important as the need for the information.

Key features of access controls include the process of validating identities, verifying the authenticity of the user or the system, and granting/denying authority to requested actions. The primary strengths of each phase are in the sense that access is possibly restricted, yet, each access control mechanism has inherent weaknesses. For example, easy to use passwords--many people will select a password that is easy to remember, but also easy to identify by individuals wishing to violate the system.

A system is at substantially greater risk if access control does not address who has read-only, write-only, or read-write privileges. Users should be restricted to a specified type of access.

Weaknesses in access controls emphasize the need for careful management. In many organizations, this management becomes the responsibility of the internal auditor, data administrator, or other such manager.

B. *Encryption*

Encryption protects data from unauthorized access by use of algorithms or coding. Recovery of original data is possible only through the use of these methods. Several standard algorithms include transposition, product, or substitution of characters. Public key encryption involves coding and is used on networks.

C. *Personalized Access*

Personalizing access to electronic funds transfers (EFT) with Personal Identification Numbers (PIN) has been the primary access control method used by financial institutions. Other organizations have begun to follow suit, as increased security is provided by combining initial access via cards, or other means, with a personalized number.

1. **Cards and PINs**

Access via cards, with or without PINs, created opportunities and threats for security. There are opportunities to improve security in the system because a personal card must be physically available as well as a PIN. Threats include theft of the card and PIN. The initial threat is the direct intrusion into the funds of the original owner; the second threat is a spill-over effect to individuals who begin denying transactions that were made. The spill-over effect occurs as the initial fraud is disclosed publicly.

The accountant/auditor helps in the management and control of cards and PINs. Management and customers must be educated as to the importance of security. A lost or obsolete PIN can be dangerous in the hands of the wrong person, as fraudulent transactions do not take much time or effort to be initiated. Therefore, changes, re-placements, and deletions of cards and PINs must always be handled in the must secure manner.

2. **Physical Identifiers**

Certain physical characteristics are thought to be unique to each individual. Fingerprints were the first characteristic used to identify a person. Recent progress in digitizing fingerprints has given systems security specialists an opportunity to use fingerprints as employee access controls. It is unclear whether customers would be willing to participate in such access controls, or whether it would even be practical. Other characteristics used include earlobes, voice prints, handwriting, retinas, and size and shape of hands.

D. *Audit Trails*

Access controls must be monitored for their utilization, strengths, and weaknesses. The audit trail gives a recording of system usage and abuses of access controls.

1. **Accounting**

The accounting audit trail records data origin and types, and system assess activities. Items recorded include:

a. *User identities*
b. *Validation routines used*
c. *Access and usage desired*
d. *Physical location of originating site*
e. *Session times and dates*
f. *Access methods and number of tries*
g. *Results of access: authorized or rejected*

2. Operations

Operations audit trails identify how well controls are working, hindering access, and consuming system resources. The number of denials may indicate unauthorized attempts, or difficulty with access protocol--access controls may hinder access. Access controls can be measured and facilitate cost/benefit ratio analysis to determine system resource consumption.

VI. INPUT CONTROLS

The purpose of input controls is to permit entrance of only authorized and accurate data into the system. This may take at least two forms:

- Initial or raw data that the system is to process, or
- operating instructions for the system to perform.

In either case, effective and efficient reentry requires validation and a corrective process. Increased use of shared data and system resources necessitates the strongest input controls. The accountant/auditor must be constantly attentive to minimizing possible weaknesses, and maximizing strengths of these controls.

A. *Data*

Data is the lifeblood of the organization. Without data, no organization could survive long. Before the advent of electronic forms, input devices, and transfer mechanisms, data originated only in paper-based documents, and controls utilized a paper trail. Electronic input controls are now part and parcel of the system and are initiated automatically, and therefore must become part of the audit trail.

1. Preparation

A key element of the data entry process, regardless of the automation used, is the preparation of the data. The automation process transfers data preparation process elements to the system.

a. *Conversion to Machine-Readable*

The primary data preparation technique converts original input to machine-readable format. Tapes, disks, cassettes, cards, and other such originating media may even need additional conversion beyond the machine readability. Please note that the key to the data conversion process is to eliminate the need for human intervention. Techniques such as bar codes and scanners are part of the trend to minimize data entry errors.

b. *Prepare Totals*

A control total is established, via various calculations of document entries, to measure the system result. The number of invoices or documents is often used as a hash total to verify that the correct number of documents were reviewed.

c. *Human Scanning as Quality Control*

The test of reasonableness is used as a control strategy. Experienced individuals visually scan data to detect errors that might have been missed, for a variety of reasons.

d. *Verification*

Either the system or a machine eventually has to convey whether or not the data is acceptable. A verification statement releases the data to the system for use by any and all authorized users.

2. Gathering

The physical gathering of data must be managed. Three sources of data are:

a. *Paper-Based*

Data that originate on paper documents require paper-based controls and a conversion process to machine-readable format. (A paperless society does not seem to be in the foreseeable future.)

b. *Machine-Based*

The environment for machine-based data gather is improving with the development of touch screens, touch telephones, voice recognition, and so forth. Edit and validation routines enable immediate problem recognition and correction.

c. *Mixture*

A mixture of machine-based and paper based data gathering is becoming prevalent as bar codes and scanners become a norm. Point of sale terminals enable the sales transaction to up-date local inventory records, sales histories, compensation, and reordering information. Input controls are critical to the system using instantaneous machine-capture.

3. Review

Validating and reviewing the data is an integral part of input controls. This review may be done via human and/or machine. The key is that a control must exist before entering data into the processing stream.

a. *Components*

Components of the review process include human interaction, machine interaction, data analysis techniques, and machine scanning, such as optical character readers.

b. *Design*

Each component must be designed with the objective of data control in clear perspective. A set of results must be determined before designing source documents. For example, the accountant/auditor must consider:

- What data to gather,
- How to gather the data,
- Who will gather the data,
- When the data will be gathered, and
- How the data will be handled, retained, and used.

Design of an invoice requires attention to input control mechanisms, even if the invoice is totally electronically generated and linked to and from vendors.

4. **Controls**

Control totals are the total number of forms, or items, entered. This serves as a check against the entry of all forms, or items.

a. *Hash Totals*

Hash totals are calculated for any element in the form, or data entry cycle. For example, the stock number of every item on an invoice may be totaled, then this total used as a check total for the data gathering invoice total.

b. *Financial Totals*

Selected financial items from any data gathering source are used to calculate financial totals. Thus, financial totals of the prices, extensions, and overall totals provide a check for accuracy of the data gathering process.

c. *Document Counts*

Documents may be counted to validate the set of documents, thereby ensuring the completeness of data gathering. This process is often described as a physical check over the batch.

B. *Validation*

Validation implies that the gathered data is correct and accurate from the appropriate source. The goal is to intercept the error before the system acts upon it, or the system is activated.

1. **On-line**

On-line validation allows immediate review as close to the origin as possible. Master files and application programs are necessary to perform the validation.

2. **Batch**

Batch checks are used to verify that all necessary entries have been made and are comprehensive. Examples include control totals, transaction review, sequential numbers, and size aspects.

3. **Lexical**

Lexical checks are used to evaluate each word, symbol, or figure entered when compared to an application-specific vocabulary.

4. **Semantic**

Semantic checks are used to validate that the applications produce the expected results based on limitations intended.

5. **Syntactic**

Syntactic check are used to validate the detail order of the program. That is, calculations should occur in a certain order. Additionally, mathematical calculations require numbers and the syntactic and semantic checks validate that such commands are justified against numbers only; otherwise, an error message occurs.

6. **Corrections**

Errors may be reported on the screen, or by hard copy. In either case, an established routine must be in place to rectify the situation. Efforts should be made to correct the cause of the error and not just the error itself.

C. *Error Controls*

Errorless systems would be nice, unfortunately, errors are a fact of life in systems. Given this reality, and the pervasiveness of the problems that error can cause, management and the auditor must decide together the controls necessary to address any given error. Risk analysis and cost/benefit analysis are used to assess the extent to which controls need to be installed, the measures needed to eliminate the error, and the source of errors.

1. **Error Report**
   Error reporting is imperative to the error control process. On-line errors should be reported immediately, and corrective action taken or the reason for not taking corrective action noted. Reporting errors is insufficient by itself; the error control process demands that corrective action be monitored. Errors may be identified through a series of checks, some of which include error handling routines.

2. **Field Checks**
   Field checks include validating and checking data in a certain field. Variables examined include omitted data, letter/numbers, acceptable limits of range set for the field, acceptance of the check digit if used, and other such items relative to the field.

3. **Record Checks**
   Record checks include validating and checking the relationships between fields. This includes the test of reasonableness, the consistency of positive ad negative signs, acceptable sizes, and ordering (certain fields should be accessed in a particular predefined order).

4. **Batch Checks**
   If a physical batch of transactions is created, then a batch check can verify that the appropriate number of entries was made. For example, is a batch of accounts receivable invoices contained 121 invoices, there should be a batch check at the end of the run to validate that 121 invoices were entered.

5. **File Checks**
   File checks are routines that validate that the proper files have been accessed and updated. Errors such as accessing or updating the wrong file, the wrong version of the file, or etc., may present serious restoration problems if not adequately addressed.

VII. COMMUNICATION CONTROLS

The communication system moves data, files, and applications from one system, or subsystem, to another. Asset safety and data integrity are of primary concern.

A. *Risks*

Data may be destroyed, temporarily misplaced, or the subject of terrorism in its broadest sense.

1. **Reliability**
   The communications system must be monitored for its ability to accurately and reliably transmits and receives data. Inaccurate data transmission is referred to as data corruption. Data corruption most frequently originates from interference on the communications lines, though there are various other sources.

2. **Unauthorized Uses and Abuses**
   The communications system is most vulnerable to unauthorized uses and abuses, and requires protection by proper authorization and access controls. Due to extensive systems networking and connectivity on a global basis, this issue will continue to be a major concern of management, accountants, and auditors.

3. Errors
Communications system errors may occur due to the laws of physics operating on the system in the form of heat, noise, electricity, or other physical manifestations. Management must continually review and improve the quality of transmission resources.

B. Technical Failure
Components may fail. Attention must be paid to the mean time between failure (MTBF) when estimating the risk of component failure.

1. Communications
Communications lines, or media, may fail. A modem may lose, or corrupt, data. Efforts to monitor the quality of the transmission via modem, or other devices, is an ongoing challenge. A series of checks and balances can be used to detect errors, but this requires the use of substantial system resources and increases a vulnerability for other errors to be introduced.

2. Hardware
Power failures, disk crashes, and power surges are typical hardware failures. Uninterruptible power sources and redundant hardware are available devices to correct such failures.

3. Software
Failure of an operating system and application system could be a catastrophe for an organization; regular backups reduce the effects.

4. Personnel
Management and operation personnel may fail, or reduce their efforts, at keeping the communications system operational and secure. Careful investigation and monitoring of the communications personnel is an integral part of the system.

C. Terrorism and Other Overt Threats
Terrorism is defined as the overt, hostile act by an external or internal intruder to the system.

1. Aggressive
Aggressive acts are behaviors that modify the data or results in the system.

a. Insertion
Terrorists may add messages or data to a system to cause changes for personal benefit, or merely to challenge the system. Transactions may be inserted by anyone, once into the system.

b. Deletion
Deletion is when the intruder destroys data or transactions. Deletions may be directed to the intruder's accounts or data, or they may be a more malicious and random attack to the system. In the latter case, an audit trail for altered accounts will not be of benefit.

c. Modification
Terrorists may change the value of specific data. For example, the dollar amount of a payable may be altered to someone's advantage.

d. Intervention

Terrorists may act as an intermediary in a system. He might deny access, or edit data or transactions. In certain instances, the sender and receiver may not be aware of the intervention.

2. Non-intrusive

Other acts, though not as intrusive as terrorism, threaten the integrity of the system and can cause serious system degradation if left unattended.

a. Note or File Sending

Hackers often perceive that note and file ending is not as damaging to a system as other acts. Yet, the possibility that a 'worm' or virus might seriously damage the system is very real. One example is the recent case of a student who inserted a runaway note into the electronic mail system from a university site.

b. Monitoring Activities

A less aggressive act is one of monitoring the system for activity. By identifying the sources and recipients, a competitor may identify trends that reveal elements of a business strategy or possible changes in business efforts.

3. Controls

Many controls that are general to systems controls are needed to address communications systems controls. Specific controls for communications systems include denying physical access, and disabling an effort, if the system is penetrated. Control of overt acts can be address by encryption or keying code numbers.

One control requires a response from the sender. In this environment, the purpose is to determine if the sender or receiver is authorized and valid.

a. Audit Trail

This audit trail traces all messages through all nodes by identifying sources, receivers, nodes, times, dates, and in some cases, data itself.

b. Operations Audit Trail

This audit trail uses operating documentation to trace data input and output instructions.

VIII. PROCESSING CONTROLS

Processing system controls include those that enhance the reliability of the CPU (central processing unit), the memory (real or virtual), the operating system, and the application programs. Each of these components have controls relative to their access, utilization, effectiveness, and efficiency.

A. CPU Controls

Although the accountant/auditor has relatively little to do with the CPU, there are a number of issues that may be addressed relative to the performance monitoring aspects of the system. Performance monitoring and tuning is a term used to denote the analysis and review of the configuration and runtime of the system with the intent to optimize the access, storage, processing, and output functions. The accountant/auditor is involved mainly to avoid postponed upgrades and capital investments because of system performance tuning. Specific controls include:

1. **Instruction Set Check**
   An instruction set check validates that the program instructions are executable. The CPU will not attempt to reuse the invalid code again and again.

   Another instruction set check validates that a specific instruction is permitted to be executed. This is critical if a particular instruction might affect the value limit in a specific register, and thus permit improper updates or access to data.

2. **Status Check**
   A status check control identifies and confirms that an instruction may be implemented. Some instructions have pervasive effects, and should be performed by only specific people and processes.

   a. *Kernel*
      The kernel is the most central and critical part of the operating system. Access to it must be severely limited and controlled.

   b. *Supervisor*
      The supervisor state is the next most critical aspect. From this state, all instructions other than kernel instructions may be invoked. Control is vital.

   c. *Problem*
      The problem state is the more usual state in which user developed and invoked programs are implemented. Only a limited set of instructions are valid in this state. Control is vital in this state in the sense that state changes must not be easily made from this state to a more critical state.

B. *Memory Controls*
Memory controls are directed towards identifying electronic errors, controlling access to memory, and preventing access to designated memory from unauthorized programs.

1. **Physical**
   Physical controls that monitor electronic fluctuations in memory are vital in assessing the degree of reliability of the CPU. One approach is to check a stored parity bit with the parity of the current contents of the memory location.

2. **Access**
   Access to real memory is carefully monitored to prevent the contamination of the operating system and any programs running in memory. In addition, access to real memory must be managed to prevent idle capacity problems.

3. **Virtual**
   Virtual memory controls validate the request for virtual memory as the allowable size and that the requested action is within the permissible actions.

C. *Systems*
Both operating systems and application systems require extensive controls. With shared data and other computing resources, it is vital that the systems be controlled. Risk assessment of these vital systems is critical in an EDP audit.

1. **Operating**
   Operating systems allocate the computing resources and in essence provide the initial level of security. If the operating system has been violated, the entire system is at risk. No application control may be sufficiently compensatory to offset such a violation.

Auditors must become aware of the possible violations in each specific operating system of interest. These violations may be initiated by people with an in depth knowledge of the system and its vulnerability. Yet, these same people are the ones with the expertise to advise and assist the auditor in examining the controls inherent and needed.

a. *Protected from Users*
The operating system must have a control to prevent users from intervening in the operation of the system. Access must be limited in such a way as to protect the operating system as well as data to which access is sought.

b. *Insulated from its Environment*
The operating system should have appropriate controls to systematically shut the system down in a catastrophic situation. Each operating system section or routine should not be able to contaminate any other section or routine.

c. *Users Isolated from Each Other*
No user may be permitted to contaminate another user's programs or data. Users cannot be permitted to contaminate their own sections or routines.

d. *Examples*
Most examples of fraudulent intervention in the operating system involve some form of disguise. That is, the instigator attempts to trick the system, the operator, or the user into thinking that the instigator is legitimate.

2. Application

Application systems carry out user commands and programming instructions that do the actual 'computing' application. To the extent possible, application systems must have controls built in rather than added on. The accountant/auditor must have early and continuous input into the control structure of application systems.

a. *Validation Reviews*
Validation reviews of the mathematical calculations are designed to assess the accuracy, completeness, and legitimacy. Alphanumeric or alphabetic reviews are less clear in that the processing is minimal but involves the actual replacement of data in fields.

b. *Programming Reviews*
Programming controls are designed to assess the extent to which good programming structure has been used. Elements of programming controls include rounding routines, programming automation (minimal human involvement), mathematical routines, and avoidance of assumed values.

c. *Interfaces among Programs/Routines*
Many programs provide input to subsequent programs. Control is critical in these interfaces as the passing of bad data can create pervasive errors. For example, a purchasing system interfaces with the inventory and accounts payable systems, and then links with the general ledger system. An error in the early part of the cycle becomes pervasive. For this reason, interface control is another critical element of the overall security policy.

3. Audit Controls

Audit trails and replication methods should enable the auditor to reprocess any transaction or process on any data. Operating or management audits are needed to monitor the access and utilization of the processes in order to assess and plan resource consumption.

IX. DATABASE CONTROLS

Databases and database systems are the basic framework for current systems in most organizations. Specialized database hardware and software is available. Database structures are available that permit the effective and efficient use of data in ways previously contemplated but never operationalized. With this kind of knowledge power, the issue of controls is critical.

A. *Access to Levels*

Only legitimate users should be able to access data in the database. Access needs to be limited by level to ensure that access is granted on a need to know basis and that restrictions apply to the instructions that may be carried out.

1. Name

Users may be restricted to certain data names and to the privileges they may carry out.

2. Content

The content boundaries of the data may limit the user's access and privileges. For example, a personnel user may access salaries of less than $80,000; a marketing representative may access customers in a certain state; and a manufacturing representative may access product information except for invoice prices.

3. Context

Access to restricted data may be authorized or not depending on the context in which the access is sought. That is, access may be granted if the particular request is one in which the control goal is not violated.

4. History

History controls are used if a sequence of instructions might overcome the restrictions of access controls. Thus, an user might issue sequential instructions at different times that accomplish the goal. Clearly, this control is not easily to develop and institute.

B. *Application Oversight*

The database must be protected in order to ensure the integrity of the data and the database management system. The application system is the contact with the database system for providing instructions and details regarding errors or unusual occurrences.

1. Update Policy

Update controls are oriented to validating the changes in the database so that they are consistent with the physical reality that the database represents. The primary controls are checks on the completeness of processing of the transaction file and the master file.

2. Reporting Procedures

Reporting controls are used to alert the user to possible inconsistencies. Listings or some form of control total may be used to request the user to validate that the system remains in control.

C. *Concurrency*

Shared data and computing resources create advantages and disadvantages. One key disadvantage is the issue of multiple users seeking access and updates at the same time. If the system locks out a user or process when this is encountered, a situation known as a 'deadly embrace' may freeze the system.

1. **Replication**
   Careful attention must be given to distributed databases as well as to multiple users accessing simultaneously. In some systems, the database is copied and one copy is designated the primary copy. Users seek access to this primary copy as the main throughput for the system. This process may cause its own set of deadly embrace problems as well as update sequencing problems. All copies must be locked before updating.

2. **Partitioning**
   In a partitioned database access is controlled via a routine that locks the data for either read or write. The lock for the write function effectively clocks out other access and on all replications.

3. **Priorities**
   There are many control issues in database concurrency and deadly embrace that affect all goals of the audit. Cost benefit analysis is the approach to use to evaluate the alternatives and to assess the extent of control versus management flexibility. With the increasing pervasiveness of database systems, it is imperative that the accountant/auditor participate fully in discussions that examine the planning and control of these database systems.

D. *Encryption*

Because of the extremely important and proprietary nature of data in a database system there may be a need for encryption of the data. Special concern must be placed on data that is moved from one database to another and the degree of reliance placed on the transferred data.

1. **Transportability**
   Data that is frequently moved may require automatic encryption to minimize the negative consequences if the data is lost or stolen. This offers little or no protection from internal theft as the encryption code would be the same for each machine or storage device.

2. **Personalized**
   If relatively little data sharing occurs, then the individual user can personalize the encryption code.

3. **Multiple levels of Access**
   If sharing is needed and security is critical, then a multiple level approach may be used. The multiple level approach pertains to the fact that multiple codes may be used, each at a different level. Thus, users have access to the key that is appropriate for their level.

E. *Physical Security*

Physical protection of the database is needed in the form of restricted access to the database storage area, the actual database systems that are operational, and other key database items.

1. **Access**
   Access to the storage and working area must be restricted to those with a need to be there. Individuals must be carefully screened before assignment there and frequent reviews of the security are necessary.

2. **File Protection**
   As mundane as it may seem, database tapes need to be identified in order to prevent accidental erasure or write over. Special consideration must be given to the use of internal as well as external labels on the tapes.

3. **database Administrator (DBA)**
   The DBA is in charge of the database but does not necessarily have the authority to override security. Thus, the DBA may not have the authority to execute the database; rather the DBA provides policy analysis and direction for the database. Note this careful distinction, the DBA may not have the actual power to 'run' the database but instead concentrates on the design and other policy issues.

4. **Backup**
   The grandfather, father, and son (grandmother, mother, and daughter) approach is used to make backup copies. This does require physical storage and capacity considerations.

F. *Audit Controls*

An audit trail must be maintained that permits the re-creation of the database at any point. Thus, there must be date and time record of each transaction, there needs to be a capture of the before and after value of the particular item affected in the database, and there must be a mechanism provided to update the audit trail itself in the event that a process was out of control temporarily and has been corrected.

From a performance standpoint there needs to be a record of the resources accessed and used in the operation of the database. By identifying the usage, the accountant/auditor or DBA may find ways of improving the productivity of the system and the organization.

Finally, the accountant/auditor and DBA work together to ensure the successful security arrangements and the successful recovery of records as needed. These are probably the most complex of all controls since the entire transaction set may have to be re-created.

X. OUTPUT CONTROLS

The output system consists of the approaches, presentation mode, and timing of the output of the system. Both data integrity and asset safety are important along with effectiveness and efficiency. In general these controls are oriented to timely production for those users granted access and restriction of the output from who are not granted access.

A. *Production*

Production of output must be monitored to ensure the timely creation of reports or other needed form of output. At the same time not every user can get their reports as needed due to scarce resources.

1. **On-line**
   On-line controls must be in place to prevent unauthorized users from accessing, using, or modifying the output. Some of these controls use rules to maintain the restrictions placed on selected data. For example, if someone is attempting to deduce the account balance of a particular client but only has authority to examine the averages of the client balances, then a series of queries that lead to the deduction must be prevented. These controls are not easy to install and maintain as there seems to be a way to get to the data regardless.

Another way of controlling access is to modify the result of a query with some random or specific algorithm in order that the exact nature of the data is not revealed. Of course, this does result in an accuracy decline.

On-line controls such as these vary in their capabilities to secure data, their degree of accuracy, and their cost benefit results.

2. Off-line

Off-line controls are somewhat more secure in the sense that there is a timelapse between the request for information and the resultant delivery. Attention must be made to the physical security of these off-line reports as the reports tend to accumulate in a central area leaving them vulnerable to unauthorized access.

Reports need to be designed to represent the organization and to be cost effective in their execution. Thus, cost benefit analysis must be undertaken to design reports and their distribution process including printing requests. These controls include such items as titles, degree of security, disposal routine, and page numbering.

Even the forms and other printed materials must be controlled. Pre-numbered forms are especially vulnerable to unauthorized use. Careful inventory methods must be used to ensure the security of critical forms such as invoices and checks.

If systems output is not immediately printed, it may be spooled to a form of temporary storage for later printing. This temporary storage must be protected from intrusion as files may be edited or read without authorization. Control over the spool is exercised via management controls as well as close review of the console log. As the spool or batch is printed, there should be controls in place to ensure the proper number of copies and runs have been made. Certain reports require such security that the console operator is not permitted to review the materials.

3. Ad Hoc

Ad hoc output is the more difficult output to control as not every eventuality is foreseen. Controls over ad hoc reports is needed to ensure that the on-line and off-line security controls are not circumvented by an unauthorized request via the ad hoc or irregular report request.

B. Distribution

Reports are not just generated but they are in fact distributed to decision makers in the organization. All four goals are of concern in the distribution of reports: asset safety, data integrity, effectiveness, and efficiency.

1. Physical Requirements

As noted above, the essence of controls in this area is to limit access and modification of the reports. The critical issue in many instances is to educate personnel in the nature and value of the reports. Of course, the use of controls is vital, too.

2. Control

Given the earlier discussion on access, retention, and modification controls, additional controls are needed in the areas of quality control and output removal. Someone needs to edit the output for missing data and other errors without compromising the integrity of the output. Output removal routines must be established with the same goals as there have been sufficient instances of trash/garbage searching to reveal the information potential in the garbage can.

C. *Presentation*

Information and output without presentation is similar to a tree falling in the forest with no one there to hear it. Plus, it does seem to matter in which form the output is presented; that is, the information communicated may be affected by the mode of presentation. Thus, controls over presentation are needed.

1. **Content**

Content controls represent the controls over which data items are included in a report. The essence of these controls is that someone has made a decision (directly or acquiescent) about the data to be included. Content controls cause managers to think directly about the data and their inclusion or exclusion. Variables to consider include the age of the data and the number of time periods over which the data are accumulated, the extent to which detailed accuracy versus reasonable accuracy is necessary, the degree of aggregation versus disaggregation, and the extent to which the data is condensed. Each of these variables may have an effect on the decision made; thus, controls to minimize bias and distortion are needed.

2. **Physical Form**

Physical form controls are intended to match the form with the intended results of ease of use and minimization of errors in use. The paperless society still seems some distance away; yet, the fact of matter is that society is using alternative output media other than paper but we simply are processing more data. The choice of paper, computer terminal, voice output, or other form of output such as microfilm or microfiche is essentially a cost benefit decision.

3. **Format**

Format controls are needed to establish standards regarding color versus monochrome and regarding tables versus graphs. Color and graphics have intuitive appeal but academic research has failed to find any consistent relationship with productivity or quality. Yet, management seems to prefer color and graphics; given their preference and resources dedicated to their delivery, it is incumbent on the accountant/auditor to monitor the investment and the results. This way, management can at least be alerted to possible resource reallocation or biased decision making because of the format.

4. **Layout**

Layout controls affect the placement of data or information on the screen or the report. Because the placement location is the primary determinant of response time and response time is a contributor to user satisfaction, there are excellent reasons for managing and monitoring the layout function.

Layout also affects the perception of importance and clustering of data: early items are perceived to be more important and clustered items are perceived to be similar.

5. **Time Aspects**

Output controls regarding time address the issue of when to print or deliver output. Because management has a preconceived notion of the correct time delay, careful attention must be paid to this preconceived notion. In some instances it may be necessary to build in some time delays just to manage the expectations of the users. In other instances it may be necessary to build in messages about the status of the task in order to appear active to the user.

D. *Interpretation*

Output in and of itself is of no value without interpretation; yet, management may not be able or choose not to interpret the output by themselves. In either case the user is confronted with the responsibility of interpretation.

1. **Availability**
   The availability of interpretation assistance is critical to decision makers who need it. This assistance may be in the form of help screens or in the form of a person. The issue of availability must be addressed by the accountant/auditor for two reasons. One, the need for availability needs analysis and confirmation. Two, the quality of the interpretation needs evaluation.

2. **Warning System for Further Information**
   An integral part of the interpretation is the need for further information to be easily determined and accessed. The output should indicate the degree and nature of additional information that may be needed.

XI. EVIDENCE

Accountants/auditors and managers deal with evidence regarding situations. Thus, it is no surprise that evidence is sought in the examination of controls. Evidence is sought to confirm or disconfirm the degree to which controls are in place to help the system to achieve the four goals identified at the beginning of this module.

A. *Needs*

The reliance of the organization on the systems in modern society lends credence to the fact that the system is the nervous system of the organization and vital to survival and success. At the same time of this importance, there are no organizations with unlimited resources; thus, cost benefit analysis must dictate the allocation of resources to the EDP audit. Systems or components with high risk need special attention. Risk matrices may be prepared in which the risks to the business are associated with various systems. Audit goals may be identified from among the following:

1. **Assess Quality of Data**
   Accountants/auditors should evaluate the extent to which the data in the system is comprised of the expected types and quality. Should the data be of lesser quality than expected, reviews of the system, the developers, and the users should be instigated.

2. **Evaluate Processes**
   The quality and quantity of data revealed may indicate a processing problem. Regardless of the data quality, an assessment is needed of the processes. Both generalized audit software and parallel simulation assist in this assessment. The key component of this assessment is to remember that one of the goals is to aid management in decision making; therefore, the processes should provide information that is useful and timely.

3. **Review Existence of Processes and Data**
   In some instances it is necessary to confirm the existence of processes or data. For example, does the system provide an inventory obsolescence report, an accounts receivable aging report, or similar report? If it does, the accountant/auditor needs to

sample the reports for selecting a set of items or accounts for further review and verification.

4. **Initial Review**
   As the accountant/auditor begins the audit, careful attention must be paid to getting the facts together. In many cases this simply means getting current on the business environment and current strategies.

   a. *Analytical Review*
      Analytical review is technique used to examine the financial ratios of the organization over a period of years within the organization as well as a comparison to industry ratios and trends. This review is designed to give some initial signals to areas of concern.

   b. *Statistical Analysis*
      Selected statistical functions may be necessary in the completion of a particular audit. For example, if a financial institution is experiencing substantial loan losses, the accountant/auditor may need to use a discriminant analysis subroutine in the audit.

   c. *Spreadsheet*
      Most audit tools are centered around the use of a spreadsheet. This provides for standardization among auditors and audit tasks as well as permits the downloading of data from the system to a workstation or PC.

   d. *Expert Systems or Decision Support Systems*
      Many accountant/auditors are finding expert systems and decision support systems to be effective and efficient tools in the context of an EDP audit. Tools such as these minimize the raw number crunching or data analysis and permit the auditor to concentrate on the larger issues. An example is the use of a PC-based expert system that prompts a relatively inexperienced internal auditor through a series of questions on internal control and then prints a draft report for the internal auditor to share with the auditee.

B. *Limitations*
As always, there are no clear and clean solutions to the audit question. What is clear is that the accountant/auditor must address these issues in a logical and cost beneficial manner. In doing this, the accountant/auditor recognizes the limitations of the environment.

1. **Often After the Fact**
   Much of auditing takes place after the fact; thus, controls in place and functioning on a regular basis are key variables to success. The need for concurrent auditing tools and techniques is increasingly evident but their use is still somewhat experimental.

2. **Constrained to Extent of generalized audit software**
   (GAS) Most of the processes and limitations noted above are part and parcel of generalized audit software. Yet, generalized audit software can only do so much. Unless programmed to do so, the GAS will not test for extreme values or conditions in the transaction set. No GAS can address all changes and deviations that may occur.

C. *Generalized Audit Software*
Given the above comments on GAS, what is GAS and what can it do? GAS is software written in a sufficiently high programming language that accountants/auditors may use it in numerous hardware and software environments. Basic functions include access to files,

sorting routines, arithmetic and statistical routines, classification mechanisms, and reporting capabilities. More specialized functions include:

1. **Parallel Simulation**
   Parallel simulation involves the writing of a program to emulate the application itself. Then the live data are processed and the results checked. Careful attention must be given to discrepancies as they may indicate an error in the parallel simulation program or in the application program.

2. **Integrated Test Facility**
   The integrated test facility actually embeds a test deck of data into the processing system. As one might expect there is a necessity to identify the transactions from the integrated test facility. After all, these fictitious transactions are being run through the system; purging of these transactions is necessary before final reports are provided from the system. This approach does permit the testing of all extremes of transactions and control processes.

3. **File and Record Extraction**
   Some GAS have extremely specialized file and record extraction routines that are sufficiently complex to permit the auditor to sort, combine, and analyze the files and records in any desired manner.

D. *Specialized Audit Software*

Specialized audit software is available to address most audit environments. As usual, the auditor is confronted with a cost benefit dilemma regarding their use.

1. **Industry Specific**
   Industry specific audit software is available that is configured to address the top two or three application programs used in an industry. Thus, the accountant/auditor may make high level requests of the GAS and their execution is immediate. This minimizes the effort of the auditor in developing requests for a non-industry specific audit software.

2. **Configuration Specific**
   Even more specific is audit software that is intended for use with a particular hardware and software configuration. This approach allows the auditor to make extensive use of the capabilities of the system and of the audit software that are somewhat integrated.

3. **Potential to be More Efficient**
   The auditor has a substantial opportunity to be increasingly efficient in using specialized audit software. Attention must be paid to the tradeoff between the cost of the specialized software and its inherent capabilities to address the audit questions.

4. **Less Flexible Than GAS**
   Given these advantages of specialized audit software, the primary disadvantage is the decline in flexibility.

E. *Concurrent Techniques*

Concurrent auditing techniques address the problem of the after the fact audit by inserting audit programs into the applications program to either collect data or to test controls with fictitious data. Continuous review of complex systems may be a cost effective way of monitoring the system and its controls.

1. **Concurrent Integrated Test Facility**
   The concurrent integrated test facility is oriented to continuous monitoring of the system and requires extensive controls of the ITF to prevent contamination of the live system. By inserting dummy but controlled transactions into the system, an auditor may validate the controls and processing of the system on a timely basis.

2. **Simulations**
   Parallel simulations run in the application systems and the simulations to be discussed here can run in the database system. By modifying the database system, a more efficient environment is created for on-line audit controls.

   a. *Continuous*
      The continuous aspect of this concurrent technique is that the simulation is active at all times. This activity is oriented to examining each transaction and determining if it meets the criteria for further examination or is ready for processing. Exception reports are the primary communications from such a simulation.

   b. *Intermittent*
      The intermittent aspect of this concurrent technique is that the auditor can change a parameter in the simulation to invoke additional checks of controls and of transactions.

3. **System Control Audit Review File (SCARF)**
   SCARF is a concurrent technique with data capture capabilities. The auditor can select the points at which data will be selected for the SCARF. Typical data collected include errors in the application system, errors in the application of the requirements of management policies and procedures, exception reporting, statistical sampling routines as needed, and operational performance data. SCARF tends to be a concurrent technique with elements of after the fact review by auditors.

F. *Human Techniques*

Evidence is collected to the extent possible by automated systems but human techniques remain an important component of the overall evidence collection process. After all, systems work is still composed of humans and machines.

1. **Interviews**
   Interviews are usually one on one communications with interested parties to a certain event. The intention is not to stress the interviewee but to obtain information in a cooperative manner; interrogatories are best left to those most skilled in handling adversarial communications.

   a. *Preparation*
      Successful interviews begin with proper preparation. Background research on the topic at hand is critical in order to avoid wasting the interviewee's time. Outline the interview topics in order to avoid unnecessary stress during the interview and to cover the topics needed in the time allotted.

   b. *Observation*
      Careful observation during the interview permits the interviewer to identify potential follow-on questions. Basic professionalism should apply in the sense that the interview results do form a portion of the total evidence collected regarding a system. Some interviews are being tape recorded or videotape recorded but these

techniques tend to formalize the responses; if necessary, these techniques should be used in carefully selected situations.

c. *Evaluation*

The interviewer should immediately prepare notes of the interview. If additional information is needed, this is the time to get it. Are there disconfirming or confirming items relative to the control objectives for which the evidence was sought. If necessary, the auditor may initiate additional evidence collection procedures in new areas previously not investigated.

2. Questionnaires

Since there is insufficient time to do everything, the auditor can use questionnaires for additional evidence gathering about controls and systems effectiveness and efficiency. Questionnaires are similar to interviews in that planning is critical.

a. *Determine Objectives*

A questionnaire cannot address everything so the auditor must determine the objectives and focus the questions on the objectives. The objectives give direction to the respondent base and thus ensure that the right personnel are given the questionnaire. The objectives also determine the type of responses requested: facts, opinion, response scales, and other details.

b. *Plan Questions*

Questions should be planned that when answered give the evidence that was desired. Questions should be direct and specific in order to minimize any 'read in to them' problem. Use questions that stand the challenge of time in the sense that someone looking at the questionnaire in the future could identify the issues and see the essence of the questionnaire.

c. *Test*

Before administering the questionnaire, test it on a small sample of other auditors and potential respondents. This provides an opportunity to refine the questionnaires before any mass distribution has been done.

d. *Deliver*

Manage the distribution of the questionnaire with oversight to the expected return date and expected response rates. Decide on a follow-up procedure and develop protocols that maximize the response rate with minimal intervention on the part of the auditor.

e. *Analyze*

Finally, analyze the data and determine if the questionnaire results support the objectives sought. Develop notes and refinements to future questionnaires. If appropriate, some statistical analysis may be necessary; careful attention needs to be paid to the correct theoretical development if this analysis is pursued.

3. Observation

The auditor may participate as an observer in two ways: participant or observer. In so doing, the auditor is attempting to collect evidence in the most direct manner on the way the system operates as well as in the people operate with the system and its controls.

a. *Work As Participant*

The auditor as an active participant must be careful to pull a fair share so as to avoid any disruptions in system operations. The advantage to this approach is that the auditor has an opportunity to work with the system on a 'live' basis.

b. *Unobtrusive*

The alternative observation mode is to be an unobtrusive observer. The difficulty with this approach is that the auditor may see or notice all the nuances that actually take place or the personnel will behave as if they are being observed as opposed to working normally.

G. *Flowcharts*

Flowcharts provide a schematic of the system and its control features. Patterns may be recognized that indicate a strength or weakness. Flowcharts may be used during the development phase to identify and suggest control points.

1. **Document**

The document flowchart is used to identify the documents, their decision points, and their distribution. By eliminating all comments except for the associated controls a document control flowchart may be generated.

2. **Data Flow**

Data flow diagrams show the flow of data through the system. By eliminating all comments except for the associated controls a data flow control flowchart may be generated. This aids the auditor in understanding how data integrity is maintained.

3. **Systems**

Systems flowcharts show the flow at the physical level among the typical components of the system such as communications, processors, storage, etc. A systems control flowchart aids the auditor in understanding the risk of contaminated data in the entire system.

4. **Programs**

Program flowcharts provide insights into the details of a program. Auditors can identify control points that may or may not lead to control weaknesses that are inherent to the program.

H. *Machine Techniques*

System efficiency evidence may be collected by monitors that are linked or embedded into the hardware and software of the system. Successful review of the evidence may permit increased efficiencies to the extent that an upgrade or an expansion may be delayed (This is analogous to an increase in capacity.).

1. **Hardware Monitors**

Hardware monitors are included in the hardware or attached to the hardware to monitor electrical impulses. These monitors are easily attached but need careful analysis to the exact point of attachment to avoid damage to the system. They do not track software performance.

a. *Tracks Activity*

By measuring the electrical impulses in the system, the monitor may track any such activity in the system.

b. *Analyzes Activity*

The hardware monitor may be programmed to provide an analysis of the hardware performance. The auditor may then make recommendations to improve overall hardware performance.

2. Software Monitors

Software monitors are subroutines built into the system to gather data on the system performance. They may be inserted into either the operating or the application systems.

a. *Internal to System*

By being internal to the system, the software monitor collects data at a detailed level relative to the hardware monitor. Typical data collected include: number of accesses, time used, sequence of events, etc.

b. *Particular Transaction versus Sampling*

Software monitors use particular transactions as the trigger point for data collection or they use a sampling strategy developed to meet the evidence collection goal.

c. *Analyzes Activity*

Software monitors have analytical capabilities similar to hardware monitors. The auditor is interested in identifying significant deviations from what is expected and determining if the needed controls are worthwhile.

XII. INTEGRATION

The auditor must bring all the issues discussed above together and give an ‘opinion’ or report to management on the status of the EDP function. Careful attention to the multiple and sometimes conflicting goals must be paid by the auditor or the audit may be successful but the ‘patient’ or the system died.

A. *Asset Safety*

Asset safety may be measured by the expected value of the loss if the asset is stolen, altered, or misused. Offset against this potential loss is the cost of the controls necessary to manage the probability of loss.

1. Measurement

Measuring these potential losses and controls is no easy task. The auditor uses probabilistic analysis to assess these items. Quantitative analysis is inadequate by itself.

a. *Qualitative*

Qualitative data must be evaluated to get a total picture of the control situation. In the final analysis, the auditor combines all the evidence and makes a final judgment on the issue at hand.

1) QUESTIONNAIRES

Questionnaires may be used as described above; in addition, the auditor may use a questionnaire to establish the record that all relevant questions were asked.

2) RISK MATRIX

Risk matrices may be used to indicate the degree of risk to the organization or to a particular system if a control is absent or not working properly. These qualitative data are combined in a quantitative fashion to derive a risk factor. The risk factors are evaluated to determine if the extent of vulnerability of the particular control or system. Resources are then allocated to the most vulnerable items.

b. *Quantitative*

Quantitative techniques are used to convert the qualitative assumptions into a meaningful number for decision making.

1) EXPECTED DOLLAR LOSS VERSUS COST OF CONTROLS

The primary calculation made is to compare the expected loss with the cost of controls. As both these numbers involve assumptions it is usually prudent to conduct a sensitivity analysis.

2) EXPECTED TIME LOSS

The expected dollar loss may be supplemented by information about the expected time loss to be incurred if the assets are not safeguarded.

2. Cost-Benefit

Cost benefit has been mentioned many times in this module. Given a perfect world, there would be no need for controls or there would be sufficient resources to institute all controls necessary to secure the data and systems. This is not to be, so auditors and management must work together to build and use the control system. In conducting a cost benefit analysis, the auditor must examine two kinds of benefits: cost displacement and value-added. Cost displacement pertains to the costs removed or reduced by implementing the system or the control. Value-added benefits are those benefits that are not as easily identified as cost displacement but are important to the strategic success of the organization.

B. *Data Integrity*

The auditor assesses the extent to which the system has protection of and for the data.

1. Measurement

The auditor must measure the integrity of the system regarding data.

a. *Qualitative*

Questionnaires and judgment are used to derive the qualitative measure. Interviews are conducted to provide additional information.

b. *Quantitative*

Most quantitative techniques mentioned earlier apply here. The key thing to remember is that the quantitative results are directly derived from their assumptions.

2. Cost-Benefit

As noted earlier, cost benefit analysis is the key to establishing and instituting controls

C. *System Effectiveness*

Systems do not run forever; in fact, they tend to degrade. Thus, an evaluation of the system effectiveness is needed. Did the system meet its stated objectives? Are there improvements that are necessary? What have we learned that we can use in future systems?

1. Objectives

Organizations have myriad objectives and goals. The auditor must recognize this multiplicity of goals in assessing system effectiveness. Overall system effectiveness has at least the following elements: economic, task, technical, operational, and quality of life.

a. *Goals of Firm*
The goals of the firm include but are not limited to short-term profitability, long-term profitability, market share, growth, human resource measures of success, or societal and managerial goals. The auditor must recognize which goal or goals are being used to assess the degree of system effectiveness.

b. *Usage*
Systems effectiveness has used usage as a surrogate for systems success. Unfortunately, unless the results are carefully evaluated the auditor may be misled by using this measure alone.

c. *Types of Usage*
Because the system may be used in a variety of ways, attention must be paid to the ways the system is used or caused to be used. Certain systems must be used while other systems have a more voluntarily nature.

d. *User Satisfaction*
User satisfaction may be an important measure of the system effectiveness. Yet, no universally available questionnaire is found; each firm must build or modify a questionnaire to meet their purposes. This does not diminish the importance of assessing user satisfaction as a component of system effectiveness.

e. *Technical*
The auditor assesses the degree to which the information architecture, hardware, and software meet the needs of the system in supporting the goals of the organization.

1) HARDWARE
Hardware effectiveness uses the evidence collected by hardware monitors and other forms of evidence if needed. Selected overall measures may be used; for example, what was the average response time, was the system down or up when users needed it?

2) SOFTWARE
Software effectiveness uses the evidence collected by software monitors plus the information gleaned by examining maintenance logs, program change request documents, and runtime and storage usage.

3) DEGREE OF INDEPENDENCE OF COMPONENTS OF SYSTEM
Because of the need to meet future uses and goals, hardware, software, and data need to be independent. This creates a tradeoff situation, as integrated systems may not possess the independence appropriate to the control needs.

2. Judgment
Because of the complexity of situations and the need for decisions, the auditor must make a decision about system effectiveness. Consideration must be given to all information gathered and then a decision rendered.

3. Overall Evaluation
Based on the above judgment about system effectiveness the auditor provides an overall evaluation to management. A variety of techniques may be used to assist the auditor. These techniques include checklists, decision support systems, expert systems, and sharing insights with other auditors or information systems professionals.

D. *System Efficiency*

As system components became increasingly inexpensive management tended to permit continued investments without evaluating system efficiency. The current environment calls for cost control and efficiency measures before increases in systems budgets.

1. **Objectives**

   Objectives for the system efficiency review should include whether the objective is general or specific plus note any assumptions. The system efficiency review may include more than just system usage. Some items include relative ease of use, trend lines in productivity, and other such performance measures.

2. **Indicators**

   Efficiency indicators are quantitative expressions of input/output measures. These indicators give a standard by which previous performance, expected performance, and alternative performance may be evaluated.

   a. *Workload Monitors*

      A variety of workload monitors or modules are available. The concept is that the auditor can select the approach consistent with the goal of the audit or review. In some instances these modules become test bed checks to evaluate system performance.

   b. *Systems Checks*

      The system itself may need to be checked for efficiencies. One way is as above where modules are used. Another way is to build mathematical or analytical models and evaluate their theoretical efficiency with comparisons to the actual systems.

3. **Overall Evaluation**

   Given the evidence collected the auditor must make a recommendation regarding the overall system efficiency. Judgment is called for as in the above discussion.

E. *Summary*

Finally, the auditor comes to the end of the line and a recommendation is necessary. This recommendation may be in reference to the entire system or a component.

1. **Qualitative**

   The auditor evaluates the qualitative evidence as an integral part of the audit process.

   a. *Collect All Items*

      The auditor collects all items and not just easily obtained or understood items. This means that the qualitative evidence collection process is critical to providing an audit trail of the logic used.

   b. *Think*

      The auditor then thinks about the implications of the qualitative data about the goals of the assignment.

2. **Quantitative**

   The auditor evaluates the quantitative evidence as an integral part of the process given the goals of the audit.

   a. *Financial or Business Terms*

      In many instances the quantitative and qualitative evidence will require translation into financial and business terms beyond the initial quantitative terms used for evidence collection. This mandates the auditor to be cognizant of the business relationship to the system and allows management tot exercise management control over the system.

b. *Sensitivity to Assumptions*

The auditor must assess the degree to which the system is sensitive to assumptions. This permits an informed judgment regarding the nature and implications of the quantitative evidence.

3. Judgment

Auditors make judgments; regardless of the particular situation, an auditor must make a judgment and justify it on the evidence and experiences in similar situations. Given the uncertain and qualitative nature of systems evaluations, it is no surprise that auditors want as much assistance as possible from others as well as from expert systems or other tools.

a. *Group Decision Making*

Auditors may prepare briefs for presentation to other auditors and managers in order share their preliminary judgments and to gain insights from others. Special attention must be given to the issue of group consensus since it is not universally true that a group consensus is necessarily correct.

b. *Experience Transfer*

Based on all the above the auditor must endeavor to integrate all evidence and processes into a cogent and rigorous analysis on which to make a recommendation to management. Then the auditor must transfer the experience in one audit to subsequent audits through documentation and/or through the development of expert systems. In addition, the auditor should prepare documentation suitable for assisting future auditors in performing EDP audits.

Teaching Considerations

SUGGESTED SCHEDULE

The following sample module plan is based on the offering of twelve to fifteen hours of lectures with outside laboratory and homework time. Any of the following may be selected to supplement the course materials.

I.	**GOALS**	**1 hour**
II.	**ROLES.**	**1 hour**
III.	**SYSTEMS CYCLE**	**1 hour**
IV.	**GENERAL INTERNAL CONTROLS**	**2 hours**
V.	**ACCESS CONTROLS**	**1 hour**
VI.	**INPUT CONTROLS**	**2 hours**
VII.	**COMMUNICATION CONTROLS**	**1 hour**
VIII.	**PROCESSING CONTROLS**	**1 hour**
IX.	**DATABASE CONTROLS**	**2 hours**
X.	**OUTPUT CONTROLS**	**1 hour**
XI.	**EVIDENCE**	**3 hours**
XII.	**INTEGRATION**	**2 hours**

HOMEWORK AND LAB EXERCISES:

The following are suggested examples of possible exercises that enhance the lecture material for this module.

1. Class/Paper exercises:
   a. Assess the roles played by managers and auditors in a specific organization. Compare notes from one organization to another. Why do they differ or why are they similar?
   b. How are input controls used in the organization with which you are most familiar?
   c. Conduct a research project on the amounts and types of computer abuse present in a particular industry. How do industries vary in their risk profiles?
   d. Provide examples of how an auditor might integrate quantitative and qualitative evidence in order to form an opinion.
2. Lab exercise
   Develop a conceptual plan for demonstrating strong and weak controls. Provide a plan for prototyping such a project for subsequent students.

Bibliography

1. Canadian Institute of Chartered Accountants, *Computer Audit*
2. Guidelines (Toronto, Canada: Canadian Institute of Chartered Accountants, 1975).
3. Canadian Institute of Chartered Accountants, *Computer Control Guidelines* (Toronto, Canada: Canadian Institute of Charted Accountants, 1970).
4. Chambers, Andrew D., *Computer Auditing* (London: Pitman Books Ltd., 1981).

5. Clowes, Kenneth W., *EDP Auditing* (Toronto: Holt, Rinehart and Winston of Canda, Limited, 1988).
6. Cornick, Delroy L., *Auditing in the Electronic Environment: Theory, Practice and Literature* (Mt. Airy, Maryland: Lamond Publications, Inc., 1981).
7. Davis, Keagle W., and Perry, William E., *Auditing Computer Applications: A Basic Systematic Approach* (New York: John Wiley & Sons, 1982).
8. Davis, Gordon B., Adams, Donald L., and Schaller, Carol A., *Auditing & EDP* 2nd ed. (New York, American Institute of Certified Public Accountants, 1983).
9. Edwards, John D., *Accounting and Management Controls for Computer Systems* (Sydney: CCH Australia Ltd., 1980).
10. FitzGerald, Jerry, *Internal Controls for Computerized Systems* (San Leandro, California: E.M. Underwood, 1978).
11. Halper, Stanley D., Davis, Glenn C., O'Neil-Dunne, P. Jarlath, and Pfau, Pamela R., *Handbook of EDP Auditing* (Boston, Massachusetts: Warren, Gorham, & Lamont, Inc., 1985).
12. Hsiao, David K., Kerr, Douglas S., and Madnick, Stuart E., *Computer Security* (New York: Academic Press, 1979).
13. Jancura, Elise G., and Boos, Robert V., *Establishing Controls and Auditing the Computerized Accounting System* (New York: Van Nostrand Reinhold Co., 1981).
14. Krauss, Leonard I., and MacGahan, Aileen, *Computer Fraud and Countermeasures* (Englewood Cliffs, New Jersey: Prentice-Hall, Inc., 1979).
15. Leiss, Ernst L., *Principles of Data Security* (New York: Plenum Press, 1982).
16. Parkinson, M. J. A., and Paul, R. G., *PC Taming: The Audit and Control of Microcomputers* (Canberra: Institute of Internal Auditors and EDP Auditors Association, 1987).
17. Porter, W. Thomas, and Perry, William E., *EDP Controls and Auditing*, 5th ed. (Boston: Kent Publishing Company, 1987).
18. Sardinas, Joseph L., Burch, John G., and Asebrook, Richard, *EDP Auditing: A Primer* (New York: John Wiley & Sons, Inc., 1981).
19. Stanford Research Institute, *Systems Auditability and Control: Control Practices* (Altamonte Springs, Florida: Institute of Internal Auditors, 1977).
20. Fernandez, Eduardo B., Summers, Rita C., and Wood, Christopher, Database Security and Integrity (Reading, Massachusetts: Addison-Wesley Publishing Company, 1981).
21. Vasarhelyi, Miklos A., and Lin, Thomas W., *Advanced Auditing: Fundamentals of EDP and Statistical Audit Technology* (Reading, Massachusetts: Addison-Wesley Publishing Company, 1988).

Articles and Other Materials

1. Abdel-khalik, A., D. Snowball and J. H. Wragge (ASW), "The Effects of Certain Internal Audit Variables on the Planning of External Audit Programs," *Accounting Review*, April 1983, pp. 215-227.
2. Ball, L. D. and M. L. Fetters, "Accounting Disclosures Requirements Impact Software," *Infosystems*, 1/83, pp. S/30-S/32.
3. Cash, Bailey and Whinston (CBW), "A Survey of Techniques for Auditing EDP-Based Accounting Information Systems," *Accounting Review*, Oct. 1977, pp. 813-832.
4. Connor, J. E. "Control System Priorities for the '80s," *Management Accounting*, March 1983, pp. 48-51.
5. Davis, G. B. and R. Weber, *Auditing Advanced EDP Systems: A Survey of Practice and Development of a Theory*, MISCR, Limperg Institute, 1983, pp. 45-73.

6. Dean, M. "How a Computer Should Talk to People," *IBM Systems Journal*, Vol. 21, No. 4, 1982, pp. 424-453.
7. Deloitte, Haskins & Sells (DH&S), "SEC's Spencer Discusses Impact of Computers on Disclosure Rules," *The Week in Review*, 12/17/82, pp. 2-3.
8. Ferrey, J. B. "Auditing the Operating System," EDPACS, April 1983, pp. 1-8.
9. Hansen, J. V. and W. F. Messier, Jr. "Expert Systems for Decision Support in EDP Auditing," *International Journal of Computer and Information Science*, 1982, pp. 357-379.
10. IFA IAPC, "Auditing in an EDP Environment," Exposure Draft 15, 10/1/82.
11. OCIS, SCRIPT User's Guide, MUSIC Tutorial and MUSIC Primer.
12. Orsey, R. R. "Methodologies for Determining Information Flow," T*he Economics of Information Processing*, Vol. 1, Wiley, 1982, pp. 57-70.
13. Peachtree, Peachtree Accounting Series, excerpt.
14. Perry, W. E. "Using SMF as an Audit Tool--Accounting Information," EDPACS, Jan. 1975, pp. 1-9.
15. Perry. W. E. and D. L. Adams, "SMF--An Untapped Audit Resource," EDPACS, Sept. 1974, pp. 1-8.
16. PMM, System 2170 Guide (From *Accounting* (820)).
17. PMM, "T&H Wholesale Grain & Supply, Inc. Case" materials (from *Accounting* 820).
18. Reneua, J. H. "Auditing in a Data Base Environment," *J. Accountancy*, Dec. 1977, pp. 59-65.
19. Rothberg, G. B., *Structured EDP Auditing Lifetime Learning Pub*., Belmont, CA, 1983, pp. xv, 2-15.
20. Singer, M. "The Vitality of Mythical Numbers," *The Public Interest*, 1971.
21. Timnick, L. "Electronic Bullies," EDPACS, Jan. 1983.
22. Tversky, A. and D. Kahneman (T&K), "Judgement Under Uncertainty: Heuristics and Biases," *Science*, 1974, pp. 1124-1131.
23. Weber, R. "Audit Trail System Support in Advanced Computer-Based Accounting Systems," *Accounting Review*, April 1982, pp. 311-325.
24. Will, H. J. "Auditing in Systems Perspective," *Accounting Review*, Oct. 1974, pp. 690-706.
25. Yoder, S. and Knight, S. "Eight General Ledgers for Small Business," *PC Magazine*, Feb. 1983, pp. 136-164.

INFORMATION SECURITY: CAN ETHICS MAKE A DIFFERENCE?

Corey D. Schou
Director
National Information Assurance Training and Education Center
Idaho State University

John A. Kilpatrick
Associate Professor
Department of Management
Idaho State University

1991

ABSTRACT

Information is a vital organizational asset that affects ongoing decision making. It has a finite life span therefore if it is delayed in its distribution, it has reduced value; if a proper user fails to have access, the information has no value. The objective of attempts to secure the organizational information system is to see that unauthorized use is not possible, that destructive viruses are not introduced, and that unauthorized study and alteration of records and files does not occur during the distribution of data and information throughout the organization while guaranteeing that proper users have easy access to their information. Are these objectives strictly technical problems, or is it possible and appropriate to broaden the scope to include the ethical issues that are raised as the security system is developed and installed? The argument in this paper is that it is both appropriate and necessary to consider the broader issues.

INFORMATION SECURITY: CAN ETHICS MAKE A DIFFERENCE?

Introduction

Information is the lifeblood of an organization that over the years has become recognized as an asset. Although determining the value of this asset from an accounting standpoint is difficult, it should be protected like any other. One of the dominant characteristics facing any firm attempting to become and to stay competitive is the dependence on information processing that relies on computers and computer software. In this paper we attempt to address many of the ethical issues facing managers in organizations as they attempt to cope with the complexity and cost of acquiring, integrating and securing information systems in the workplace. In large organizations, this task is assigned to an Information Resource Manager who is responsible for all aspects of information processing from data entry to the Executive Information System.[2] This manager plays an important role in the security of the organization's information assets. It is critical that Information Resource Managers convey the importance of resource security to senior management of the organization.

In the process of performing this task, the manager must balance two competing objectives that are for all practical purposes antithetical. The first is that of ease of access to information to meet the requisite variety needs of decision makers within a system.[3] The second is that of maintaining security, confidentiality and privacy of organizational information assets.

Frequently, this process is viewed as a technical problem rather than the more complex socio-technical problem that should address some of the following issues:

- Whose rights are to be considered?
- To what extent are these rights in conflict?
- What are the responsibilities of the information specialists?
- How honest and trusting are the members of the user community? In what sense do they represent a 'community'? What are the implications, if any, of their holding certain interests in common?
- How trusting ought they to be? What is implied in the use of the term *ought*? Of the term *trust*?

These socio-technical problems are fundamental ethical issues. These issues may or may not be legal issues. The manager should be aware that which is legal is not necessarily a logical equivalence of either ethical or right.[4]

2 Schou, Corey D., "Computer Security: Training Needs for Managers," *Data Security Management,* Auerbach, September, 1990.

3 Beer, Stafford, *The Brain of the Firm*, John Wiley & Sons, New York, NY, 1981.

4 Richards, T., Schou, C.D. & Fites, P.E. "Information Systems Security Laws and Legislation," in *Information Technology Resources Utilization and Management: Issues and Trends,* Idea Group, Harrisburg, Pa., 1990.

Questions Of Purpose And Value

Since there is a documented body of law that governs portions of our behavior and a cult of technology which asserts that it can make our electronic information systems invulnerable to external penetration, we tend to rely upon it. To complete the protection of our information assets, we must develop an awareness of value systems. This development must be more than another set of rules and regulations that dictate how we should behave. They should be, on the other hand, an internalized set of behaviors. We should ensure that rules and technology do not become the sole focus of our security activities. These are destined to fail of their own weight in the long term. John LaCarré in one of his novels makes the point about the impact of technology on human activity by stating:

> *George Smiley: "You've made technique a way of life. Like a whore, technique replacing love."*[5]

In a technological environment, it is easy to focus on the techniques designed to accomplish goals and on the technology used to assist in the accomplishment of those goals. At times the tendency is to allow the focus on technique to overshadow the purposes or ends. For example, a common observation of the modern 'rat race' (a revealing metaphor) is that participants spend so much time and energy pursuing the good life that little remains for living. As this result suggests, it is easy to become obsessed with the tools and in the process to forget the purpose of the tools.

Although information security systems are adequate from the successful system control, they do not always take into account the corresponding human impact and implications. This brings us to the question – What is the role played by the values that members of a community hold that form the choices made and the ends toward which those choices are directed? Stated another way, what is the significance of the way a member of the information systems community views the world and his or her relation to that immediate world and to other members of the community? These values and perceptions underlie the choices that individuals make, the goals that are pursued, and the priorities that are established. They affect both the means that are selected and the ends toward which efforts are directed.

Ethical Systems

What are the purposes of computer information systems? Information systems are organizational mechanisms that collect data and distribute information. Frequently these systems rely on electronic devices such as computers; however, the 'office boy' carrying a scrap of paper to the file drawer also meets this definition.

Some systems relate to governmental objectives (e.g., national defense, collection of revenue, monitoring of international trade), some to business purposes and needs (e.g., efficiency and competitiveness), but all must relate at some level to social needs and values. For example, one might argue that a fundamental value is respect for the rights of others. Another might be that the overall objective is a better quality of life for all members of the community.

5 LaCarré, John, *Tinker, Tailor, Soldier, Spy*, Doubleday, New York, NY, 1986.

There are several ways of identifying and deciding ethical issues. One of the most common Judeo - Christian ways of categorizing these approaches is the rules *Vs.* consequences criteria. The first argues that our actions should be guided by general rules or principles: do not harm; tell the truth; do not steal; have respect for persons as ‘ends in themselves.’ The second argues that we should assess the *rightness* of an action or decision by the consequences that will likely result. Most commonly the second approach identifies some value or values, and measures an action by the extent to which these values are or are not enhanced, or whether progress is made toward certain goals, such as a better life for all. From a practical standpoint it may be recognized that, for most people, over a span of time and in different situations, both approaches will be used. That is, in general some ethical rule may seem appropriate but under extreme circumstances exceptions to the rule or principle will appear ethically acceptable because of the likely consequences.

Ethics And Information Systems

For an information system to function effectively and efficiently, there must be a free flow of data and information among all participants. In the ideal situation, there would be no barriers to this flow; this would improve the probability that ‘perfect information’ is in the hands of the decision makers. Of course, for this to occur, there would have to be perfect confidence and trust within the organization.

CONFIDENCE AND TRUST

Information — adequate, relevant, timely, and understandable — is a precondition of an efficient and free society. Yet it is a means to power . . . Therefore, the rights to create property in information, to withhold, to disclose, to determine when and how disseminated are critical.[6]

In this section we are interested in the ethical issues involving the creation, control, use, abuse, dissemination, protection, manipulation or alteration, examination and destruction of information and its attendant data in computer systems. In order for the above information activities to take place efficiently and legitimately, there must be some minimal level of trust and confidence in the systems which handle the information. Is it also necessary for there to be some minimal level of trust among and between the various users of the system?

Assuming that such a level is necessary, what are the preconditions in order for this confidence and trust to exist? It appears clear that first there must be a proven and recognized history of dependability, both within the firm and with similar systems. By raising these issues in the context of the firm’s culture or atmosphere, one ethical principle is implied: that there must be respect for persons and certain property rights. This falls within the first approach identified above, which argues for the assessment of choices in light of certain ethical principles or rules. Actions which result in intrusion, examination, alteration or destruction of information belonging to others might be judged as morally wrong because they violate the principle of respect for persons. The second approach, that of looking at the consequences of an action, might suggest that in order for a community to meet the needs of its members, individuals within the community must be able to have some confidence in systems of communication. According to this view, it could be argued that actions that unduly interfere with the smooth

6 Behrman, Jack, “Information Disclosure, the Right to Know and the Right to Lie’” in Behrman, *Essays on Ethics in Business and the Profession*, Prentice Hall, Englewood Cliffs, NJ., 1988, 79.

operation of information and communication systems, or that diminish the confidence and trust in these systems, should be judged as unethical.

DEFINITIONS

As a starting point for determining ways of evaluating actions, it is appropriate to construct several definitions. The term *legitimate* is fundamental to the notion of balancing rights and responsibilities. For the purposes of this paper, it is argued that for an action or behavior affecting an information system to be legitimate, it must aid in the achievement of one or more objectives of the system without unduly interfering with progress toward other accepted objectives. The definition can be applied to the ethical management of information. One objective of the system is to provide information that is without deception and is understandable, timely, relevant, complete and appropriate to the user. Upon examination, it can be seen that this definition suggests both the practical and ethical elements of managing computer information systems.

Specific Concerns Relating To The Design Of Secure Systems

Those involved in the design of a secure information system must be aware of the conflicting rights, responsibilities and needs of system users and professionals, and of the implications of some of these conflicts. Some paradoxical assertions may serve to illustrate:

- For people to have trust in an information system, the manager must trust no one.
- Systems which are truly trustworthy must use control processes that inhibit use.

Another way of putting the problem, as Clifford Stoll suggests in his book, *The Cuckoo's Egg*,[7] is that as administrative controls are added to ensure trustworthiness, the system becomes more difficult to use. This means that the people for whom the system is designed end up finding another, less trustworthy but more easily accessible system to use. The term administrative controls refers to those policies and procedures imposed by a manager that are designed to regulate the individuals and activities covered by the policies and procedures.

Administrative controls are designed and implemented to make sure that people act in the way that managers desire. Generally this means, in ways that advance organizational objectives through fixed procedures. This may be something as simple as standardizing the ways employees claim reimbursements for job-related expenses. It may mean something as broad as the budget process, which attempts to regulate the activities of and to set standards for the entire firm. Frequently, however, it also refers to the need to regulate behavior when it is perceived that:

- a) there is motivation to engage in activities for personal, as opposed to organizational, reasons; and
- b) those activities are potentially harmful to the organization, to organizational values or to other organizational members.

If the interests of individuals always coincided with those of the organizations with which he or she lives and works, there would be very little need for administrative controls. It is at the point where these interests diverge that the need for controls arise. Further, some conflicts arise because of simple misunderstandings, some arise because of differences in perceptions, some are

7 Stoll, Clifford A., *The Cuckoo's Egg*, Doubleday, New York, NY, 1989.

due to different priorities, world-views or values, and some come about because of individual malevolent intent.

Finally, there are those instances where it is in an individual's self-interest for everyone else to exercise a degree of moral restraint while he or she exercises none. This can be seen as the *free-rider* problem or, to use Garrett Hardin's excellent metaphor, it is the "tragedy of the commons"[8]. In this environmental fable, the members of the community maintain their livestock on the commonly held grazing grounds. Animals can safely be added until the carrying capacity of the grounds are reached. However, it is to the benefit of any individual community member to add animals to his herd on the commons. The overall costs of degradation are borne by the community but the benefits accrue to the individual community member. The tragedy is that individuals can safely benefit in the short run while the long-term costs are dispersed. Greed is rewarded. One lesson for members of the community is that, unless they are willing to eliminate all cooperative efforts, the exercise of some moral restraint by each individual is necessary.

Examples Of Ethical Issues Confronted In Organizations

As long as the information system consists of 'office boys' carrying paper from place to place, the problems are less complex. If he takes something home — he has stolen — he is wrong. However, when the organization begins to rely on electronic means, this issue becomes more clouded. The same individual can take or send electronic images of the same information without overtly changing it. (After all, what is the value of a simple '0' or '1'.)The following are examples of some problems that are uniquely electronic.

PIRATED SOFTWARE

One of the more obvious and most prevalent problem deals with the use of pirated software. The temptations are obvious and the risk of disclosure is slight. Why then the concern? There are several ethical issues here, but perhaps the overriding one is that of the failure to recognize intellectual property.

As with many ethical concerns, one can arrange many positions along a continuum. In this instance, one can take an extreme individualist or ethical egoist position, and argue that pirating another's software is not a big issue, and is useful for financially strapped organizations. Further, one can argue that it is the responsibility of the developer to take measures to limit the ease of pirating. In any case, is it stealing if the property isn't gone?

At the other end is the argument that:

- there are rights that are being violated while copying;
- that no community can exist that refuses to acknowledge and protect the rights of its members; and
- that progress will be limited unless there is some incentive for individuals to develop tools that will prove useful in solving the problems of the community.

The manager then must address the issue of whether to allow - profit from - the pirating of another's intellectual creation, or, if the policy is to ensure that this does not occur within the business, what policies will be required to ensure that it does not occur.

8 Hardin, G., "The Tragedy of the Commons," *Science*, 162, December 1968, 1243-1248.

CRIMINAL ENTRY

Even if one has problems recognizing intellectual property, physical property is easier to define. This situation is analogous to the problem of the 'office boy' If someone breaks your physical lock, or physically enters your premises, there is little question about 'right'.

However, the problem of unwarranted entry into proprietary electronic information systems with criminal intent is more complex. Using technological means, each firm will obviously wish to ensure that its own system will not be so penetrated. What of information gained either inadvertently or through the wizardry of an employee who also happens to enjoy the challenge of breaking into another institution's information systems? Since any technological means of protection may be compromised by 'wizardry' it is important that one engender an atmosphere of 'correctness' within the organization.

COMPUTER SURVEILLANCE & EMPLOYEE RECORDS

In a 1931 speech, George Bernard Shaw observed:

> *An American has no sense of privacy. He does not know what it means. There is no such thing in the country.*

At the time he may have been correct; however, the American society has matured during the last sixty years. Even though Supreme Court candidates have been unable to define the absolute nature of the rights of privacy on a constitutional basis, most Americans believe that they have a vested right of privacy based on the Fourth Amendment to the Constitution[9] . This for the most part protects us from our government.

Computerization of information systems has made the communication and dissemination of information about companies and individuals an accepted procedure. The issue of computer surveillance and employee records involves questions about the uses of databases that may involve invasion of privacy, either the customer's or employee's, and employee monitoring in the workplace. This latter involves the inclusion of a piece of software in the information system which monitors and times or otherwise measures the activities of operators. Is this a legitimate managerial exercise of administrative control, or is it an unwarranted intrusion into the employee's privacy? Put another way, should the firm legitimately be concerned only with the quantity and quality of the employee's activities, or may it also surreptitiously monitor the employee on a minute by minute basis? Questions of the impact on morale aside, how far may the manager extend his or her control over the activities of the employee? The sensitivity of this issue becomes more acute when the ability to control is magnified or enhanced by the computer's capacities. One other issue in this category involves the cross-reading or matching across information systems of employee or customer records. Again, the issue involves the right to privacy of employees and customers. Formerly, this may have been an ethical concern only in firm's large enough to have extensive databases. Today, even small organizations may have the

9 Amendment IV Right of search and seizure regulated. The right of people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation and particularly describing the place to be searched, the persons or things to be seized.

computer capacity, or have access to databases that give the firm the capacity to intrude into the privacy of employees and customers.

The owner/manager of a small firm, then, is faced with many of the same ethical dilemmas that managers in large firms face. Dealing with the issues may be more difficult in that the small firm manager must be all things to all people, with little time for contemplating the complexities of the ethics of the computer age.

GAMING

An example of an issue of interest with perhaps least clear cut ethical stands is the use of company facilities for office games, such as ‘rotisserie baseball’ and ‘fantasy hockey’. Employees face an ethical choice over the extent to which such ‘enlivening’ activities can legitimately be carried on during company time.

Managers face the need to balance productivity interests with maintaining a livable working environment that is not so rigid and controlling that the quality of work life drives off good employees.

Sources Of Guidelines And Codes Of Ethics

There are a not less than five organizations that have chosen to address directly the ethical issues posed by the rapid expansion of information technology they are:

- British Computer Society,
- Institute of Electrical and Electronic Engineers,
- Institute for Certification of Computer Professionals,
- CCP and
- The Data Processing Management Association.

The Data Processing Management Association (DPMA) has developed a code of ethics and a separate ‘Standards of Conduct.’ [10]

STANDARDS OF CONDUCT

These standards are derived from the code of ethics and are specific statements of behavior that no true professional will violate. Excerpts are provided below, as examples of ethical guidelines that are being developed by industry professionals:

In recognition of my obligation to management I shall:

- Not misuse the authority entrusted to me.
- Not misrepresent or withhold information concerning the capabilities of equipment, software or systems.

In recognition of my obligation to my fellow members and the profession I shall:

- Be honest in all my professional relationships.
- Not use or take credit for the work of others without specific acknowledgement and authorization.

In recognition of my obligation to society I shall:

10 DPMA Code of Ethics, Data Processing Management Association, 505 Bussie Highway, Park Ridge Il.

- Protect the privacy and confidentiality of all information entrusted to me.
- To the best of my ability, insure that the products of my work are used in a socially responsible way.
- Never misrepresent or withhold information that is germane to a problem or situation of public concern nor will I allow any such known information to remain unchallenged.
- Not use knowledge of a confidential or personal nature in any unauthorized manner or to achieve personal gain.

In recognition of my obligation to my employer I shall:

- Avoid conflict of interest and insure that my employer is aware of any potential conflict.
- Protect the privacy and confidentiality of all information entrusted to me.
- Not exploit the weakness of an information system for personal gain or personal satisfaction.

Summary

If, due to security restrictions, an information system cannot disseminate its contents to those who need access, it fails. Technology alone does not solve the problem. It is a human problem.

It is of benefit to each user if everyone exercises discretion, judgment and professional respect for other's rights in the use of a computer information system. Each knows then that the system can be 'trusted.' It means that the system manager will be less concerned with intrusions or violations of rights and professional courtesies, respect and so on. But it also means that if an individual does desire to access another user's files, to change data, steal information, study someone else's personnel file, install a Trojan horse or release a virus, it is much easier to do so. The implicit trust in the system makes it easy for an individual user to violate that trust. Self-restraint thus can be seen as a prerequisite for any activity requiring trust.

The violation of the trust, if discovered, necessitates a higher level of administrative control, new restrictions placed on access, and that additional procedural processes be installed. The violations have caused a reduction in the efficiency and effectiveness of the system. A fundamental consideration for the manager, then, is to assess the role of trust, the desirable and achievable level of trust to be sought, and the implications of these choices for the firm and individuals affected.

This dilemma serves to highlight the ethical considerations facing the manger. For smaller organizations, it is further complicated by resource limitations, both financial and human. What balance between absolute confidence in the security of the system and completely free access for users is desirable? What are the tradeoffs between rights and responsibilities, costs and benefits implied by the security or control provisions that are contemplated? What values lie behind the choices made? As the level of security increases, and with it the consequent increase in the level of confidence or trust in the system, what other legitimate values are diminished or threatened? In general, this is the age-old question of the balance between individual and community interests. In specific terms, it is the question of how to optimize the legitimate and responsible use of computer information systems while eliminating unauthorized use and protecting the rights of users and other affected parties.

To generalize the issues raised here:

- If people will not exercise moral restraint, systems will develop controls for protection;
- The controls for protection will prove burdensome and inefficient;
- The systems will fail;
- They will still be necessary as the threat comes, not from responsible users but from ‘mavericks’ with what is arguably an essentially anti-community ethic;
- The systems will fail to be secure

USING THE MODULES TO CREATE YOUR OWN INFORMATION SECURITY COURSE

Revised August 1990
Revised May 1995
Revised February 2001

Corey D. Schou
National Information Assurance Training and Education Center
College of Business
Idaho State University

Description:
This section shows the instructor how to use these materials to create a custom course based on the contents of the *Information Security Modules.* This principle can be used for both University and industrial courses

CREATING INFORMATION SECURITY COURSES

Since Information Security is a developing discipline in the academic community, there are few academicians who have experience teaching courses in the area. As stated earlier, these modules have been designed to supplement other courses in the curriculum; an additional use of these modules is to guide the instructor in the creation of a custom course at the undergraduate level.

By using the components of the modules separately, the instructor can tailor the course to his particular expertise. Among the authors of these modules there are individuals with backgrounds in Computer Science, Information Science, Mathematics, Management, Accounting, and even International Law. Each of us teach our Information Security Courses with an individual focus.

There is a total of up to 87 hours of instructional material contained in these modules. The breakdown is:

Introduction to Information Protection .... 5 hours
PC / Workstation Security .... 4.5 hours
Security Fundamentals .... 12 hours
Laws and Legislation .... 9 hours
System Security .... 15 hours
Communications Security .... 7 hours
Corporate Security Management .... 17 hours
Introduction to Accounting Controls and EDP Auditing .... 18 hours

Since the materials were designed with redundancy, many of the components of the modules overlap. Frequently, the overlap represents a level of detail rather than a difference in content.

Sample Outline 1 – Information Assurance for Accountants

For example, an Information Security course for accounting students might be composed of:

<u>MODULE AND CONTENT TIME</u>

Part I of Module One
Information as a corporate resource .... 2 hour
Part 1 of Module Two
Ethics .... 1 hour
Part 2 of Module Three
Organizational Policies and Procedures .... 1 hour
Part 10 of Module Three
Costs and Benefits .... 1 hour
Part 2 of Module Four
Laws as tools for computer security .... 3 hours
Part 3 of Module Four
Laws as legal options for control .... 4 hours
Part 6 of Module Five
Protection Planning .... 5 hours
Part 2 of Module Six
Threats .... 2 hours
Part 8 of Module Seven
Computer Security Checklist .... 5 hours

Module Eight
All of module Eight....................18 hours

This represents as much as 42 hours of classroom instructional time. This forms the core of material for the course. It is expected that the faculty will introduce other material that is specific to his area of expertise.

Sample Outline 2 – Legal Issues

A second suggested outline might be a focus on legal issues

MODULE AND CONTENT TIME

Part I of Module One
Information as a corporate resource....................2 hour
Part 1 of Module Two
Ethics....................1 hour
Part 2 of Module Three
Organizational Policies and Procedures....................1 hour
Part 4 of Module Three
Personnel Security....................1 hour
Part 1 of Module Four
The Underlying Problem....................3 hours
Part 2 of Module Four
Laws as tools for computer security....................3 hours
Part 3 of Module Four
Laws as legal options for control....................4 hours
Part 6 of Module Five
Protection Planning....................5 hours
Part 2 of Module Five
Security Requirements....................3 hours
Part 5 of Module Five
Data Life Cycle....................2 hours
Part 8 of Module Seven
Computer Security Checklist....................5 hours
Part 2 of Module Eight
Roles 1 hour
Part 4 of Module Eight
General Internal Controls....................2 hours
Part 11 of Module Eight
Evidence....................3 hours

This represents approximately 36 hours of classroom instructional time. This forms the core of material for the course. It is expected that the faculty will introduce other material that is specific to his area of expertise.

If you have suggestion for improvement or chose to use this technique, please send your suggestions or a copy of your course syllabus to;

Corey D. Schou
Director, National Information Assurance Training and Education Center
P.O. Box 4043 Pocatello, Idaho, 83205-4043

Each summer, we will compile these teaching materials, and distribute them to interested parties.

Topic Outline Introduction to Information Protection

I. Information As A Corporate Resource.. 2 Hour
- A. Security As Part Of The Total Organization
- B. Understanding The Organization
- C. Identifying Sensitive Data
- D. Controlled Sharing Of Information And Resources

II. Basic Security Problems ....1 Hour
- A. Natural Disasters
- B. Accidental Problems
- C. Malicious Threats

III. Ethical Issues...1 Hour
- A. Ethics And Responsible Decision-Making
- B Confidentiality & Privacy
- C. Piracy
- D. Fraud & Misuse
- E. Liability
- F. Patent And Copyright Law
- G. Trade Secrets
- H. Sabotage

IV. Major Areas Of Information Systems Study...1 Hour
- A. PC/Workstation Security
- B. Security Fundamentals
- C. Information Security Laws And Legislation
- D. System Security
- E. Communications Security
- F. Corporate Security Management

Topic Outline PC / Workstation Security

I. Ethical Use Of The Computer...1 Hour
II. Computer Room Environment..1 Hour
- A. Temperature
- B. Foreign Materials
- C. Radio Frequency Interference (RFI)
- D. Power Surges And Brownouts

III. Physical Security...1 Hour
- A. Location And Construction
- B. Computer Room Access
- C. Physical Control

IV. Data Security ....1 Hour
- A. Software Control
- B. Backup Procedures
- C. Recovery Techniques
- D. Data Encryption And Access Control

V. Security Training ....0.5 Hour

Topic Outline Security Fundamentals

I. Planning .... 2 Hours

A. Security As Part Of The Total Organization
B. Understanding The Organization
C. Identifying Sensitive Data
D. Controlled Sharing Of Information And Resources
E. Specific Needs
F. Analysis And Design

II. Organizational Policies And Procedures .... 1 Hour

A. Scope Of Security Mechanisms
B. Basic Goals
   1. Prevention
   2. Deterrence
   3. Containment
   4. Detection
   5. Recovery
C. Written Management Policies & Procedures

III. Ethics And Professionalism .... 2 Hour

A. Ethics
   1. Ethics And Responsible Decision-Making
   2. Confidentiality & Privacy
   3. Piracy
   4. Fraud & Misuse
   5. Liability
   6. Patent And Copyright Law
   7. Trade Secrets
   8. Sabotage
B. Laws And Legislation
C. Professionalism
   1. The Computer Security Institute
   2. Computer Professionals For Social Responsibility
   3. Data Processing Management Association
   4. Security Management Magazine
   5. Licensing And Certification
      A. Institute For Certification Of Computer Professionals
      B. IISSCC (ISC^2)

IV. Personnel Security .... 1 Hour

A. Hiring Practices
B. Training
C. Access Rights And Privileges
D. Rules For Granting And Revoking Privileges
E. Separation Of Privileges And Roles
F. Adverse Actions
G. Termination Practices

V. Physical Security .... 1 Hour

A. Location

1. Access Versus Security
2. Rooms, Doors, Windows, Keys

B. Environment

1 Radio Frequency Interference [RFI]
2 Cooling
3 Cabling
4. Power

VI. System Security..1 Hour

A. PC & Workstations
B. Database
C. Networks And Communications
D. Operating Systems
E. Application Software
F. Systems Security
G. Systems Architecture
H. Audit And Control
I. Corporate Security Management

VII. Threats And Vulnerability..1 Hour

A. Natural Disasters
1. Fire
2. Flood
3. Brown-Outs
4. Lightning

B. Accidental Acts (Threats)
1. Disclosure Of Data
2. Modification/Destruction Of Data
3. Faulty Software
4. Residual Data
5. Wrong Parameters

C. Malicious Acts (Threats)
1. Trap Doors
2. Trojan Horse
3. Tampering
4. Snooping Or Browsing
5. Intentional Disclosure Of Data
6. Viruses

D. Locus Of Attack
1. Terminals
2. Hosts
3. Front-Ends
4. Gateways
5. Links
6. Packet-Switches
7. PC/Workstations

VIII. Data Security And Recovery ....1 Hour

IX. Control And Audit ....1 Hour

X. Costs And Benefits..1 Hour

A. Accessibility Versus Secrecy
B. Costs
   1. Money And Time For Development, Installation, Procurement, And Maintenance Of Security Measures
   2. Special Skills
   3. Performance
   4. Productivity
   5. Training Time
   6. Compatibility - Of Equipment, Procedures,
C. Benefits
   1. Precise Definition Of Requirements
   2. Value Of Information
   3. Peace Of Mind
   4. Productivity
   5. Protection From Legal Liability
   6. Protection From Loss Of Control Of Assets/Company
   7. Good-Will
   8. Privacy

Topic Outline Laws And Legislation

I. The Underlying Problem .... 1 - 2 Hours

A. Theft Of Hardware And Data
B. Fraud
C. Physical Abuse
D. Misuse Of Information And Privacy Issues
E. Issues Of Adjudication And Regulation

II. Laws As Tools For Computer Security... 1 - 3 Hours

A. Privacy Laws And Legislation
B. Intellectual Property Laws
  1. Trade Secrets Law
  2. Patent Law
  3. Copyright Law
  4. Trademark Law
C. Federal Laws
D. State Statutes
E. DPMA Model Computer Crime Bill

III. Laws As Legal Options For Control .... 1 - 4 Hours

A. License Agreements
B. Intellectual Property Laws,
  (Trade Secrets, Patents, Copyright And Trademarks)
C. Employee Non-Disclosure Considerations
D. Contracts
E. Warranties For Software And Hardware

Topic Outline System Security

I. Overview .... 1 Hours

A. Definitions

B. Background

  1. Identifying Sensitive Systems
  2. Developing A Security Program And Plan, And
  3. Training Appropriate People Concerned With Both Development And Operation Of Systems

C. Management Responsibility

II. System Sensitivity .... 2 Hours

A. Criticality

B. Sensitivity

C. Source Of Sensitivity Information

D. Level Of Sensitivity

III. Security Requirements .... 3 Hours

A. Security Policy

B. Accountability

C. Assurance

  1. Architecture
  2. Integrity
  3. Testing
  4. Specification/Verification
  5. Facility Management
  6. Configuration Control
  7. Disaster Recovery Or Contingency Planning
  8. Compliance

IV. Levels Of Security.. 2 Hours

V. Data Life Cycle... 2 Hours

A. Retention Policy

B. Destruction Policy

VI. Protection Planning.. 2 - 5 Hours

A. System Description

  1. The Physical Location Of The Equipment
  2. Types Of Data And Information
  3. Classification Level
  4. Duration And Importance Of MIS Activity
  5. Equipment Location
  6. Equipment Description By Name And Model Number
  7. Security Officers
  8. Data Processing Terms
  9. System Integrity Study

B. MIS Security

C. Communications Security

D. Information Security

E. Personnel Security

F. Physical Security

G. Contingency Plans

Topic Outline Communications Security

I. Overview ....1 Hours

A. Brief Review Of The Concepts Of Protection In Data Communication Systems And Networks From A Management Perspective
   1. Systems Objectives: Controlled Sharing Of Information And Resources.
   2. Specific Needs: Privacy, Secrecy, Integrity And Availability.
   3. Policies And Mechanisms.
   4. Assets: Identification Of Valuable/ Sensitive Data And Information.
   5. Threats And Vulnerability.

B. The Interrelationship Of Communications Security And Network Security For Interconnected Elements:
   1. Systems Connectivity
   2. Public/Private Carriers
   3. Relationship To Reliability And Dependability

II. Threats...2 Hours

A. Types Of Attacks/Failures
   1. Passive Intrusion
      A. Disclosure Of Message Contents
      B. Traffic Analysis
      C. Disclosure Of Data On Network Users
   2. Active Intrusion
      A. Modification Or Deletion Of Message Contents
      B. Insertion Of Bogus Messages
      C. Replay Or Reordering Of Messages
      D. Viruses
   3. Natural Disasters/Catastrophes/Sabotage
      A. Human Errors
      B. Fires, Floods, Brown-Outs.

B. Locus Of Attack/Failure
   1. Terminals
   2. Hosts
   3. Front-Ends
   4. Gateways
   5. Links
   6. Switches (Includes Multiplexer, Intermediate Nodes)
   7. Interconnected PC/Workstations (Includes LAN, Host-PC Etc.)

III. Countermeasures ....2 Hours

A. Encryption
   1. Private-Key And Public-Key Systems - Des And RSA As Examples
   2. Key Distribution
   3. Link Level And End-To-End

B. Authentication
   1. Node And User Authentication
   2. Passwords
   3. Message Authentication
   4. Encryption-Based
   5. Added Protection For PC Authentication Date

C. Access Control
1. Access Control Mechanisms-Control Lists And Passwords
2. Administration
D. Contingency Planning
IV. Tradeoffs - Costs And Benefits... 2 Hour

Topic Outline Corporate Security Management

I. Overview ....1 Hour
II. Development Of Security Program ....3 Hours
- A. Objectives
- B. Policies
- C. Connectivity, Corporate Structure, And Security
    - 1. Connectivity Defined
    - 2. Affect On Corporate Structure
    - 3. Security Considerations
- D. Plans
- E. Responsibilities

III. Risk Analysis.. 2 Hour
IV. Contingency Planning.. 3 Hour
V. Legal Issues For Managers...1 Hour
- A. Licenses
- B. Fraud/Misuse
- C. Privacy
- D. Copyright
- E. Trade Secrets
- F. Employee Agreements

VI. System Validation & Verification (Accreditation)..1 Hour
VII. Information Systems Audit ....1 Hour
VIII. Computer Security Checklist...5 Hours
- A. General Information
- B. General Security
- C. Fire Risk And Water Damage Analysis
- D. Air Conditioning Systems
- E. Electrical System
- F. Natural Disasters
- G. Backup Systems
- H. Access Control
- I. System Utilization
- J. System Operation
- K. Software
- L. Hardware
- M. File Security
- N. Data File Standards
- O. Shared Resource Systems Security

Topic Outline -- Introduction To Accounting Controls And EDP Auditing

I. Goals ....1 Hour

- A. Role Of The Accountant
- B. Asset Safety
    - 1. Organizational Asset
    - 2. Computer Resource Abuses
    - 3. Value Of Systems
        - A. Hardware
        - B. Software
        - C. Personnel
        - D. Operating Systems
        - E. Application Systems
        - F. Data
        - G. Facilities
        - H. Supplies
    - 4. Proprietary And Private Data
- C. Data Integrity
    - 1. Pervasiveness Of Errors
    - 2. Individual Decisions
- D. System Effectiveness
    - 1. Decision Making Value
    - 2. Timeliness
    - 3. Support For Competitive Advantage
- E. System Efficiency
    - 1. Proper Uses Of Systems And Components
    - 2. Misallocation Of Resources
        - a. Theft
        - b. Destruction
            - 1) Physical Acts Of Nature
            - 2) Physical Acts Of Persons
        - c. Disruption Of Service
            - 1) Hardware
            - 2) Software
            - 3) Personnel
        - d. Unauthorized Changes

II. Roles ....1 Hour

- A. Management
    - 1. Top Management
    - 2. Middle Management
    - 3. Entry-Level Management
- B. Information Systems Professionals
    - 1. MIS Orientation
    - 2. Data Processing Orientation
- C. Internal Auditors
- D. External Auditors
- E. Management Controls

III. Systems Cycle ....1 Hour

A. Auditor’s Involvement
  1. Concurrent Participation
  2. Ex Post Review
  3. Phases And Concerns

B. Alternative Models
  1. Traditional
  2. Prototype
  3. Socio-technical

C. Differences In Internal And External Auditors’

D. End-User Developed Systems

IV. General Internal Controls...2 Hours

A. Segregation Of Duties

B. Proper Delegation Of Authority

C. Competent Personnel

D. Authorization System

E. Documentation

F. Physical Controls

G. Supervision

H. Accountability

V. Access Controls...1 Hour

A. Strengths And Weakness

B. Encryption

C. Personalized Access
  1. Cards And PINS
  2. Physical Identifiers

D. Audit Trails
  1. Accounting
    a. User Identities
    b. Validation Routines Used
    c. Access And Usage Desired
    d. Physical Location Of Originating Site
    e. Session Times And Dates
    f. Access Methods And Number Of Tries
    g. Results Of Access: Authorized Or Rejected
  2. Operations

VI. Input Controls ....2 Hours

A. Data
  1. Preparation
    a. Conversion To Machine-Readable
    b. Prepare Totals
    c. Human Scanning As Quality Control
    d. Verification
  2. Gathering
    a. Paper-Based
    b. Machine-Based
    c. Mixture

3. Review
    a. Components
    b. Design
        1) What Data To Gather,
        2) How To Gather Data,
        3) Who Will Gather The Data,
        4) When Will The Data Be Gathered, And
        5) How The Data Will Be Handled, Retained, And Used
4. Controls
    a. Hash Totals
    b. Financial
    c. Document Counts

B. Validation
1. Online
2. Batch
3. Lexical
4. Semantic
5. Syntactic
6. Corrections

C. Error Controls
1. Error Report
2. Field Checks
3. Record Checks
4. Batch Checks
5. File Checks

VII. Communications Controls..1 Hour

A. Risks
1. Reliability
2. Unauthorized Uses And Abuses
3. Errors

B. Technical Failure
1. Communications
2. Hardware
3. Software
4 .Personnel

C. Terrorism And Other Overt Threats
1. Aggressive
    a. Insertion
    b. Deletion
    c. Modification
    d. Intervention
2. Non-Intrusive
    a. Note Or File Sending
    b. Monitoring Activities
3. Controls
    a. Audit Trail
    b. Operations Audit Trail

VIII. Processing Controls...1 Hour

A. CPU Controls
   1. Instruction Set Check
   2. Status Check
      a. Kernel
      b. Supervisor
      b. Problem
B. Memory Controls
   1.. Physical
   2 Access
   3. Virtual
C. Systems
   1. Operating
      a. Protected From Users
      b. Insulated From Its Environment
      c. Users Isolated From Each Other
      d. Examples
   2. Application
      a. Validation Reviews
      b. Programming Reviews
      b. Interfaces Among Programs/Routines
   3. Audit Controls

IX. Database Controls ....2 Hours

A. Access To Levels
   1. Name
   2. Content
   3. Context
   4. History
B. Application Oversight
   1. Update Policy
   2. Reporting Procedures
C. Concurrency
   1. Replication
   2. Partitioning
   3. Priorities
D. Encryption
   1. Transportability
   2. Personalized
   3. Multiple Levels Of Access
E. Physical Security
   1. Access
   2. File Protection
   3. Data Base Administrator (DBA)
   4. Backup
   F. Audit Controls

X. Output Controls ....1 Hour

A. Production

1. Online
2. Off-line
3. Ad Hoc

B. Distribution
1. Physical Requirements
2. Control

C. Presentation
1. Content
2. Physical Form
3. Format
4. Layout
5. Time Aspects

D. Interpretation
1. Availability
2. Warning System For Further Information

XI. Evidence .... 3 Hours

A. Needs
1. Assess Quality Of Data
2. Evaluate Processes
3. Review Existence Of Processes And Data
4. Initial Review
    a. Analytical Review
    b. Statistical Analysis
    c. Spreadsheet
    d. Expert Systems Or Decision Support Systems

B. Limitations
1. Often After The Fact
2. Constrained To Extent Of Generalized Audit Software (Gas)

C. Generalized Audit Software
1. Parallel Simulation
2. Integrated Test Facility
3. File And Record Extraction

D. Specialized Audit Software
1. Industry Specific
2. Configuration Specific
3. Potential To Be More Efficient
4. Less Flexible Than Gas

E. Concurrent Techniques
1. Concurrent Integrated Test Facility
2. Simulations
    a. Continuous
    b. Intermittent
3. System Control Audit Review File (Scarf)

F. Human Techniques
1. Interviews
    a. Preparation
    b. Observation

c. Evaluation
2. Questionnaires
a. Determine Objectives
b. Plan Questions
c. Test
d. Deliver
e. Analyze
3. Observation
a. Work As Participant
b. Unobtrusive

G. Flowcharts
1. Document
2. Data Flow
3. Systems
4. Programs

H. Machine Techniques
1. Hardware Monitors
a. Tracks Activity
b. Analyzes Activity
2. Software Monitors
a. Internal To System
b. Particular Transaction Versus Sampling
c. Analyzes Activity

XII. Integration ....2 Hours

A. Asset Safety
1. Measurement
a. Qualitative
1) Questionnaires
2) Risk Matrix
b. Quantitative
1) Expected Dollar Loss Versus Cost Of Controls
2) Expected Time Loss
2. Cost-Benefit

B. Data Integrity
1. Measurement
A. Qualitative
B. Quantitative
2. Cost-Benefit

C. System Effectiveness
1. Objectives
a. Goals Of Firm
b. Usage
c. Types Of Usage
d. User Satisfaction
e. Technical
1) Hardware
2) Software

3) Degree Of Independence Of Components Of System

2. Judgment
3. Overall Evaluation

D. System Efficiency

1. Objectives
2. Indicators
    a. Workload Monitors
    b. Systems Checks
3. Overall Evaluation

E. Summary

1. Qualitative
    a. Collect All Items
    b. Think
2. Quantitative
    a. Financial Or Business Terms
    b. Sensitivity To Assumptions
3. Judgment
    Group Decision Making and Experience Transfer

SELECTED READINGS

A Telecom Security Blanket
Sherman, James; Demlow, William
Telephony v216n10 PP.: 33,35 Mar 6, 1989
Some System Security Suggestions
Kolstad, Rob
UNIX Review v7n2 PP: 90-96 Feb. 1989
Off-Site Information Transfer Speeds Alarm System Problem-Solving
Russell, Rebecca D.
Security v26n2 PP: 60-64 Feb. 1989
Run Circles Around Your Computer Security; Viruses -- Is the Epidemic Here?
Elsbury, David C.; Zalud, Bill
Security v26n2 PP: 48-51 Feb. 1989
Computer Use and Abuse
Kluepfel, Henry M.
Security Mgmt. v33n2 PP: 72-79 Feb. 1989
Conquering Computer Viruses
Yovel, Shlomo
Security Mgmt. v33n2 PP: 64-66 Feb. 1989
The Computer Virus: Is There a Real Panacea?
Cullen, Scott W.
Office v109n3 PP: 43-46 Mar 1989
Secure Computer Network Requirements
Satya, Vishnu
Information Age (UK) v10n4 PP: 211-221 Oct. 1988
Security and Access Control Features of the VAX/VMS Operating System
Kielsky, Michael
Information Age (UK) v10n4 PP: 203-210 Oct. 1988
Personal Computer Security
Gustoff, Mark E.; Sexton, Timothy J
Information Age (UK) v10n4 PP: 195-202 Oct. 1988
Computer Viruses: A People-Related Problem
Uretsky, Mike
Employment Relations Today v15n4 PP: 265-270 Winter 1988/1989
Too Precious to Lose: Backing Up Your Data
Archibald, Dale
Nonprofit World v7n1 PP: 14-15 Jan./Feb. 1989
Libraries and Computers: Disaster Prevention and Recovery
Miller, R. Bruce
Information Technology & Libraries v7n4 PP: 349-358 Dec. 1988
The Virus Cure
McAfee, John
Datamation v35n4 PP: 29-40 Feb. 15, 1989
The Case for Continuity
Ginn, R. D.
Security Mgmt. v33n1 PP: 84-90 Jan. 1989
Artificial Intelligence Meets the Press
Gross, Daniel
Information Today v5n11 PP: 12-14 Dec. 1988
Computer Security: The Time Is Now
Irwin, Stephen T.; Bakey, Tom
Insurance Software *Review* v14n1 PP: 33-42 Feb./Mar 1989
The "Computer Virus" Danger Grows
Menkus, Belden
Modern Office Technology v34n2 PP: 38,40 Feb. 1989
New Technology Poses Challenge to Auditors
Willits, Stephen D.; Alley, Lee R.
Internal Auditor v46n1 PP: 12-19 Feb. 1989
Bank Finds Security Offerings Lacking
Bucken, Mike
Software Magazine v9n2 PP: 46 Feb. 1989
Things to Consider for an Ideal Security Match
Lewis, Barry
Software Magazine v9n2 PP: 43-45,49-52 Feb. 1989
Managing the Virus Threat
McAfee, John D.
Computer world v23n6 PP: 89-96 Feb. 13, 1989
Computers: Auditors' Friend or Foe?
Thornhill, William T.
Internal Auditing v4n3 PP: 86-94 Winter 1989
Computer Viruses: A Guide to Protecting Your Company's Systems
Cashell, James D.; Waggoner, Jeri B.
Internal Auditing v4n3 PP: 3-12 Winter 1989
Forced Entry
Healy, Thomas S.
Insurance Review v49n9 PP: 60-62 Sep. 1988
Professional Responsibility for Information Privacy
Auerbach, Isaac L.
Computers & Security (Netherlands) v4n2 PP: 103-107 June 1985
Professional Responsibility for Information Privacy
Auerbach, Isaac L.
Jrnl. of Information Systems Mgmt. v2n1 PP: 77-81 Winter 1985
The Business of Banks
Auerbach, Isaac
Bankers Magazine v167n5 PP: 79-80 Sep./Oct. 1984
Strategies For The Management Of Computer Output
AUERBACH, ISAAC L.
Jrnl. of Micrographics V10 N3 PP: 127-129 JAN./FEB. 1977
Make Information Services Pay Its Way
Allen, Brandt
Harvard Business Review v65n1 PP: 57-63 Jan./Feb. 1987
An Unmanaged Computer System Can Stop You Dead
Allen, Brandt
Harvard Business Review v60n6 PP: 76-87 Nov./Dec. 1982
The Menace of Computer Fraud
Allen, Brandt R.
Office v90n2 PP: 74,76,84,86,90 Aug. 1979
The Biggest Computer Frauds - Lessons For CPAS
Allen, Brandt
Jrnl. of Accountancy v143 n5 pp.: 52-62 may 1977
Embezzler's Guide to the Computer
Allen, Brandt
Harvard Business Review v53n4 pp.: 79-89 July-august 1975
Computer Security
Allen, Brandt R.
Data Mgmt. Vol. 10 no 2 pp.: 24-30 Feb. 72
EDP Security
Allen, Brandt R.
Data Mgmt. vol. 10 no 1 pp.: 18 Jan. 72
User-Driven Design: A New Way to Computer Creativity
Andrews, Dorine C.; Lind, Steven D.

Office v101n5 PP: 171-172,229 May 1985
Assessing the Risk for System Failure
Andrews, Dorine C.
Jrnl. of Systems Mgmt. v33n12 PP: 30-36 Dec. 1982
The Data Connection: How to Get Users and Systems Personnel to Speak the Same language
Andrews, Dorine C.
Management World v11n10 PP: 34-35 Oct. 1982
User-Friendly Password Methods for Computer-Mediated Information Systems
Barton, Ben F.; Barton, Marthalee S.
Computers & Security (Netherlands) v3n3 PP: 186-195 Aug. 1984
On the Implications of Computer Viruses and Methods of Defense
Cohen, Fred
Computers & Security (Netherlands) v7n2 PP: 167-184 Apr. 1988
An Overview of 18 Virus Protection Products; How to Combat a Computer Virus
Highland, Harold Joseph
Computers & Security (Netherlands) v7n2 PP: 157-163 Apr. 1988
Virus Defense Alert
Anonymous
Computers & Security (Netherlands) v7n2 PP: 156,158 Apr. 1988
Are We Vulnerable to a Virus Attack? A Report from Sweden
Fak, Viiveke
Computers & Security (Netherlands) v7n2 PP: 151-155 Apr. 1988
Anatomy of a Virus Attack
Highland, Harold Joseph
Computers & Security (Netherlands) v7n2 PP: 145-150 Apr. 1988
The Application of Epidemiology to Computer Viruses
Murray, W. H.
Computers & Security (Netherlands) v7n2 PP: 139-145 Apr. 1988
Computer Viruses -- A Post Mortem
Highland, Harold Joseph
Computers & Security (Netherlands) v7n2 PP: 117-122 Apr. 1988
Stamp Out Viruses!
Zier, Joe
CA Magazine (Canada) v121n7 PP: 36-39 Aug. 1988
Computer Viruses -- Part 1
Hancock, Wayland
American Agent & Broker v60n8 PP: 12-16 Aug. 1988
Sick Computers
Welter, Therese R.
Industry Week v237n4 PP: 51,55 Aug. 15, 1988
Viruses, Trojan Horses, and Other Badware: Information and Implications for Online Searchers
Clancy, Steve
Database v11n4 PP: 37-44 Aug. 1988
How Deadly Is the Computer Virus?
Anonymous
Electrical World v202n7 PP: 35-36 Jul. 1988
Computer Corner: Has Your Computer Had Its Flu Shot?
Carland, JoAnn C.
Project Mgmt. Jrnl. v19n3 PP: 15-16 June 1988
Science and Technology: Keeping Out the Kaos Club
Anonymous
Economist (UK) v308n7558 PP: 77-78 Jul. 9, 1988
Computer Security: The How and Why?
Adams, Tony
Australian Accountant (Australia) v58n5 PP: 84-85 June 1988
Antivirus Vendors Form Industry Regulation Group
DiDio, Laura
Network World v5n28 PP: 17,20 Jul. 11, 1988
Disaster Prevention and Recovery: No Vaccine to Ward Off Effects of Virus Attacks
Menkus, Belden
Computer world v22n28 PP: S8 Jul. 11, 1988
Viruses Plague Networks, Jeopardize System Health
DiDio, Laura
Network World v5n27 PP: 1,28-30,33-34,46 Jul. 4, 1988
Protection from Infection
Lammer, Peter
Systems International (UK) v16n6 PP: 75-76 June 1988
Viruses Threatening Era of Computer Freedom
Winter, Christine
Words v16n6 PP: 41-43 May/June 1988
Computer Fraud: What You Can Do to Prevent It
Brill, Alan E.
Computers in Accounting v4n4 PP: 78-86 June 1988
Thoughts and Opinions on Online Services and Computer Communications
Picard, Don
Link-Up v5n3 PP: 3,18 May/June 1988
Sick Software? Network Virus? Insurance Won't Help
Rosenberg, Robert
Data Communications v17n6 PP: 70,72 June 1988
Viruses Infect Corporate MIS
Ryan, Alan J.
Computer world v22n22 PP: 29,31 May 30, 1988
Of Viruses and Logic Bombs: Part I
Adams, Tony
Australian Accountant (Australia) v58n4 PP: 83-85 May 1988
Effective and Inexpensive Methods Exist for Controlling Software Viruses
Gibson, Steve
InfoWorld v10n19 PP: 51 May 9, 1988
What Were Simple Viruses May Fast Become a Plague
Gibson, Steve
InfoWorld v10n18 PP: 32 May 2, 1988
Some Common Sense About Network Viruses, and What to Do About Them
Ponting, Bob
Data Communications v17n4 PP: 60,62 Apr. 1988
Self-Reproduction Key to Survival of Software Virus
Gibson, Steve
InfoWorld v10n17 PP: 36 Apr. 25, 1988
Confidentiality of Data Is at Greater Risk in the Age of Laptops and Viruses
Kask, Alex
InfoWorld v10n16 PP: 34 Apr. 18, 1988
Computer Viruses Express Themselves in Many Ways
Gibson, Steve
InfoWorld v10n16 PP: 32 Apr. 18, 1988
Preventing the Perfect Crime
Anonymous
Electrical World v202n2 PP: 34 Feb. 1988
Recovering from a Computer Virus Attack
Davis, Frank G. F.; Gantenbein, Rex E.
Jrnl. of Systems & Software v7n4 PP: 253-258 Dec. 1987
An Approach to Containing Computer Viruses Pozzo, Maria M.; Gray, Terence E.
Computers & Security (Netherlands) v6n4 PP: 321-331 Aug. 1987
As AIDS Spreads, State PC Systems Are Reaching Limits
Moad, Jeff
Datamation v33n16 PP: 43-56 Aug. 15, 1987
Pest Control for RMIS Users

Tweedy, David A.
Business Insurance v21n33 PP: 27 Aug. 17, 1987
Data Physician -- A Virus Protection Program
Highland, Harold Joseph
Computers & Security (Netherlands) v6n1 PP: 73-79 Feb. 1987
Computer Viruses: Theory and Experiments
Cohen, Fred
Computers & Security (Netherlands) v6n1 PP: 22-35 Feb. 1987
The Insidious Infection
Colby, Wendelin
Infosystems v32n5 PP: 94,96 May 1985
Message Authentication and Encryption Combined
Christoffersson, Per
Computers & Security (Netherlands) v7n1 PP: 65-71 Feb. 1988
'Remember to Lock the Door': MMI and the Hacker
Roberts, William
Information Age (UK) v10n3 PP: 146-150 Jul. 1988
A Lesson in Perseverance: MIT Computer Science Professors Study Ways to Maintain Data Integrity
Pike, Helen
Computer world v22n14A PP: 10-11 Apr. 6, 1988
The 'Free and Easy' World of PCs Is in Need of a Formal LAN Security Policy
Quinn, Thomas J.
InfoWorld v10n13 PP: S4 Mar 28, 1988
Corporate, US Security Up for Grabs?
Chester, Jeffrey A.
Infosystems v35n1 PP: 24-25 Jan. 1988
Data Base Management Controls for Microcomputer Systems
Hansen, James V.; Romney, Marshall B.
Internal Auditor v44n6 PP: 44-47 Dec. 1987
Full-Time, Real-Time System Security
Minard, Bernie
Computers in Healthcare v8n12 PP: 51-57 Oct. 1987
The Network Decision
Hagen, D. Scott; Elliott, D'arcy
CMA Magazine (Canada) v61n5 PP: 49-53 Sep./Oct. 1987
Getting a Lock on Controlling Corporate Data
Steinbrecher, David
Today's Office v21n12 PP: 40-46 May 1987
Computer Security -- How to Protect Yours
Turner, Paula F.
Legal Economics v13n2 PP: 49-53 Mar 1987
Data Security
Honan, Patrick
Personal Computing v11n1 PP: 101-107 Jan. 1987
A Risky Business
de Montgailhard, Hugues Desazars
Infosystems v33n9 PP: 82 Sep. 1986
Microcomputer Security: Back to Basics
Shoor, Rita
Infosystems v33n9 PP: 44-46 Sep. 1986
Developing Standards for Protecting Electronic Financial Data
Zeitler, Eddie L.
Bank Administration v62n10 PP: 38,40 Oct. 1986
Shared PCs Are Control Headache for Firms
Kask, Alex
InfoWorld v8n33 PP: 66 Aug. 18, 1986
Micro-Mainframe Links: A Status Report
Anderson, Kevin; Bernard, Alan
Jrnl. of Accounting & EDP v2n1 PP: 61-63 Spring 1986
Microcomputer Security: Audit Problems and Solutions
Gallegos, Frederick; Basica, Daniel
Jrnl. of Accounting & EDP v1n4 PP: 49-56 Winter 1986
Strategies for Effective Microcomputer Management
Kleinberg, Eugene R.
Jrnl. of Information Systems Mgmt. v3n1 PP: 27-35 Winter 1986
Microcomputer Security and Control Awareness
O'Sullivan, Daniel F., Jr.
Massachusetts CPA Review v60n1 PP: 14-18 Winter 1986
Data Sharing and Access Protection in Business System 12
du Croix, A. J.
Computers & Security (Netherlands) v4n4 PP: 317-323 Dec. 1985
Users Finally Realize PC's Potential by Tapping Mainframe Data Stream
Caradonna, Lori
Bank Systems & Equipment v22n12 PP: 52-56 Dec. 1985
PC's from a Data Management Perspective
Iyer, Shekar
Canadian Data systems () v17n10 PP: 90-95 Oct. 1985
Strategic Planning for Data Integrity
Harold, Kevin E.
Internal Auditor v42n3 PP: 23-26 June 1985
A Shot in the Dark
Moore, Steve
On Communications v2n5 PP: 41-44 May 1985
Micro to Mainframe: The Software Connection
Snyders, Jan.
Infosystems v32n5 PP: 40-45 May 1985
Controlling Computer Losses
Musson, Melvyn
National Underwriter (Life/Health) v89n1 PP: 9 Jan. 5, 1985
Software viruses: PC-health enemy number one. (covert code latest PC security threat) (includes related article on maximizing the safety of disks)
Joyce, Edward J.
Datamation VOL.: v34 : n20 Oct. 15, 1988
Mobilizing for war against computer viruses. (column)
Perry, William E.
Government Computer News VOL.: v7 : n21 : p107(1) : Oct. 10, 1988
Mad Macs: the scoop on Macintosh viruses: their history, identification, and eradication. (includes related articles on tips for keeping your Mac virus-free and viral antidotes)
Stefanac, Suzanne
Macworld VOL.: v5 : n11 : p92(9) : Nov., 1988
Viruses and Trojans strike - but very rarely: lowering risks of downloaded danger. (dangers of hidden, destructive software bugs)
Getts, Judy
PC World VOL.: v6 : n10 : p72(2) : Oct., 1988
'Virus trial' defendant convicted. (Donald Gene Burleson)
Brower, Emily
MacWEEK VOL.: v2 : n39 : p3(1) : Sept. 27, 1988
Checkpoints against viruses. (network manufacturers produce recommendations)
Keefe, Patricia
Computer world VOL.: v22 : n38 : p55(1) : Sept. 19, 1988
Programmer convicted after planting a 'virus'. (
Donald Gene Burleson)
New York Times VOL.: v138 : n47,635 : p29(1) : Sept. 21, 1988
Secure PCs from virus attacks.

David, Jon
Computer world VOL.: v22 : n37 : p43(3) : Sept. 12, 1988
CCTA responds to departments' virus worries. (computer consultancy warns about software viruses)
Nicolle, Lindsey
Computer Weekly : n1125 : p14(1) Aug. 4, 1988
Sparse coverage for viruses: computer insurance policies inadequate in face of spreading infection. (includes related article on arrest of computer hackers)
Daly, James
Computer world VOL.: v22 : n33 : p1(2) : Aug. 15, 1988
Razor blades in Apples. (contains related articles on virus eradication efforts and possible solution software)
Coale, Kristi
MacUser VOL.: v4 : n9 : p304(6) Sept., 1988
Package offers virus cure. (Vaccine, computer software from FoundationWare)
Computers in Banking VOL.: v5 : n8 : p61(3) : Aug., 1988
Upgrade has password control, data encryption. (Watchdog 5.0, data security software from Fischer International Systems Corp.)
Computers in Banking VOL.: v5 : n8 : p64(1) : Aug., 1988
No vaccine to ward off effects of virus attack. (disaster prevention and recovery)
Menkus, Belden
Computer world VOL.: v22 : n28 : pS8(1) : July 11, 1988
Scent of money lures firms to jump on antiviral bandwagon. (computer viruses)
Parker, Rachel
InfoWorld VOL.: v10 : n27 : p30(1) : July 4, 1988
Viruses plague networks, jeopardize system health. (computer viruses) (includes related article on infamous computer viruses)
DiDio, Laura
Network World VOL.: v5 : n27 : p1(6) : July 4, 1988
Protecting against computer viruses; know your enemy.
Kane, Pamela
Lotus VOL.: v4 : n7 : p17(2) July, 1988
Newswire. (Connectivity section)
PC Week VOL.: v5 : n26 : pC5(1) June 28, 1988
Ways to battle computer viruses: safe telecommunication may be your best protection against viruses. (Telecommunications)
Fischer, Michael
A+ VOL.: v6 : n8 : p81(2) Aug., 1988
A Virus Carries Fatal Complications. (Strict security may prevent tampering, but the stricken have little hope) (The Executive Computer) (column)
Lewis, Peter H.
New York Times VOL.: v137 : n47,548 : pF11(1) : June 26, 1988

DACUM II

DRAFT

National Information Assurance Training and Education Center

Idaho State University

Center Report 154

Description: ETCORP/Paradigm (DS) FINAL Day 5

Extract Date: 8/11/93 14:16:35

Edited 8/11/93 - Schou 14:19:33 -23:19:15

Edited 8/12/93 - Schou 08:06:31 -22:20:11

Edited 8/13/93 - Schou 05:36:01 -19:19:58

Edited 8/14/93 - Schou 06:53:33 -20:22:03

Imported Documents

Literacy and Basic Skills (78.33)

Green Book Materials (61.50)

Edited 8/22/93 - Schou 00:03:49 -02:46:23

Print Date: 8/22//93 02:56:05

Edited 11/27/93 - Schou 02:33:54 -19:03:22

Prepared by
Corey D. Schou
Simplot Decision Support Center
and
James Frost, Herb La Fond, Nathan Wingert
Simplot Decision Support Center

August 1993

DACUM II REPORT

Introduction

As a result of the Computer Security Act of 1987[11], government agencies have identified over 50,000 sensitive systems. Individuals who are operationally involved with these systems are required by the 1987 act to receive security training. The National Institute of Standards and Technology (NIST) is entrusted with the major program responsibilities for government wide computer security and their initiatives have increased the awareness and improved management and application of technology to government security. In addition, many companies have recognized the need to meet the spirit of this requirement as well. One conservative estimate is that the private sector need for information and computer security is at least twice the governmental need.

As we all know, the United States Federal Government is characterized by a large number of competing agencies with complex agendas. An example of this complexity is shown by a recent Office of Personnel Management (OPM) regulation that outlines the training requirement for the Computer Security Act.

The December 4, 1991, edition of the Federal Register announced that effective January 3, 1992[12], the heads of Federal agencies are to provide computer security training as outlined in the National Institute of Standards and Technology (NIST Computer Security Training Guidelines).

The mandated training is to be provided:

- to all new employees who fit one of five categories of computer users, within 60 days of their appointment
- whenever there is a significant change in the agency information security environment or procedures or when an employee enters a new position which deals with sensitive information.
- as computer security refresher as determined necessary by the agency based on the sensitivity of information that the employee uses or processes.

This training must be provided by all agencies and many Federal contractors. The spectrum of end users extends from the Post Office to the Department of Defense — The Department of Education to the Department of Energy.

How should one go about identifying the critical training issues? This was defined in NIST Special Publication 500-172 by Mary Anne Todd and Constance Guitan. During 1992 NIST and the NCSC convened a meeting at the Simplot Decision Center at Idaho State University. The objective was to review the Todd model in the area of awareness and to develop awareness materials for use by FISSEA[13].

---

11 P.L. 100-235

12 Under U.S. Code 5 CFR Part 930 subpart C.

13 FISSEA—Federal Information Systems Security Educators Association

The following are the preliminary results of the second Design a Curriculum (DACUM[14] II) sessions held at Idaho State University. The DACUM was conducted over a six day period during August 1993.

The meetings were conducted by the staff of the National Information Assurance Training and Education Center in the Simplot Decision Center. All data were collected using the Paradigm software package (v 1.5.3). All materials from DACUM I (1992), including the 'Green Book', were available to all participants as on-line documents. In addition there were over 15Mb of other documents for participant use. As the teams worked on the various aspects of the project, all pervious writing was made available to the entire team.

The Process

The ETCORP[15] (Electronic Technology for Collaboration, Organizational Re engineering and Paradigm Change) process used in the Simplot Decision Support Center is designed to allow individuals to work anonymously in parallel.

DAYS 0 THROUGH 3 - ESTABLISHING THE FOUNDATION

The first two days were devoted to establishing a baseline to approach the Todd model. During the third day, the teams completed the prototype of the new matrix and collectively developed a writing strategy.

First, we extended the agreement on the differences among Awareness, Training, and Education (AT&E). The following was developed as the baseline[16].

Awareness

Awareness is at the lowest level of the AT&E solution to information security. It is designed to affect short term memory. It is composed of stimulation, focus, attention, decision and assimilation. A successful AT&E program will begin by meeting these five requirements.

Stimulation

Stimulation is the very first phase of learning. At this level some event triggers a basal level response that "wakes up" the individual's nervous system. In many work places, placing a security violation notice on the boss' desk manages to get him stimulated quickly. However, that is negative stimulation. Positive stimulation is preferred. This is achieved by a variety of techniques such as distributing an announcement of cash awards for security suggestions. An example of a key for widespread recognition is to use a colored paper or a style of announcement that is unique only to monetary awards for security suggestions.

Focus

Obtaining learner focus is a concept that is not so foreign to most of us. One of the most common examples of focus is the use of different color badges to indicate specific levels of security clearance. A common example for stimulating focus is the use of different color paper

14 One characteristic of ETCORP DACUM exercises is that they are open-ended. We expect to have suggestions made to this living document.

15 ETCORP (Electronic Technology for Collaboration, Organizational Re engineering and Paradigm Change)

16 It was based on an paper presented at the 1993 IFIP conference, 1993. "Developing Awareness, Training, and Education: A Cost Effective Tool For Maintaining System Integrity", Proceedings, IFIP 1993, Canada, Schou, C.D., Maconachy, W.V.., Frost, James.

while maintaining the same shape and design for security information products that may change on a yearly basis.

Many agencies or companies use COMPUSEC information cards that are of a particular color, e.g., blue. When the content of the cards is updated, the cards are deliberately changed to a bright yellow so that users, who have these cards by their computers know just by color if their cards are current. The idea behind this form of motivation is that seeing a specific shape or color or hearing a particular tone will trigger senses to tune into the next stage of awareness – focus.

The problem with focus is that humans tend to practice a tuning out process called acclimation. If a stimulus, which was once a powerful attention getter is used repeatedly in the same environment the learner will selectively tune out the stimulus.

Attention

Attention can also be obtained by using such 'gimmicks' as key chains, magnetic tags, posters, and other visual clues that offer daily reminders that security is a work habit.

Decision

The first three steps outlined above usually take place in the human brain in a nanosecond. Once the learner's attention is attained, the leap to conscious decision becomes a critical yet most important part in changing the employee behavior. The security world abounds in examples of primary decision making behavior (often termed the exercise of short term memory). Two key control operations, use of personal passwords and inserting employee card with PIN numbers, are examples of primary decision making behavior. The purpose of imposing this level of effort on an employee is to make him think about what he is about to do.

On a higher plane, forcing the employee to exercise short term memory is necessary to evoke a higher level of security practices. These practices include:

1. Stopping to read a bulletin board or scrolling electronic messages
2. Deciding to read a new security regulation
3. Deciding to read the security corner of the company newsletter
4. Deciding to attend a security lecture

Messages developed for employees at this level are often the most difficult to construct, yet they are the key to leading an entire organization into a better security performance profile. A possible motivator is the inclusion of documented system intrusions or 'data thefts' from other firms.

Assimilation

Assimilation is a term we have borrowed from the learning theorist Jean Piaget. It is a transformational component of learning through which all knowledge is acquired. It is a cognitive process in which an individual incorporates new experiences into already existing schema of operation. At this level of operation, the learner/employee consciously decides to incorporate security practices into his behavior. This experience is characterized by a growth in behavior pattern often without significant qualitative change in cognitive processing.

Training

There is a gray zone between awareness and training as depicted earlier in figure 3. A gross distinction between them is that in awareness activities the learner is a passive recipient of information, while in the training environment the learner has a more active role in the learning process. A primary role of awareness programs is to motivate employees/learners to move into a training mode and actively seek more knowledge. A fundamental goal of training programs is to motivate learners to move knowledge and skills from short term memory into long term memory. Very often these knowledges and skills become chained sequences of behavior that require little higher level mental processing.

In organizations where these functions are divested, collaboration between the corporate providers of training and the corporate planners of INFOSEC awareness is essential to developing and delivering quality learning experiences.

TRAINING *VS.* EDUCATION

The distinction between training and education can be made by examining the intent and scope of the instruction. In a training environment the employee is taught to use specific skills as part of exacting job performance. In an education context the employee would be encouraged to examine and evaluate not only skills and methods of work but fundamental operating principles and tenants upon which job skills are based. The employee is using internalized concepts and skills to perform operations such as analyses, evaluation, and judgment to reach higher cognitive level decisions that lead to the accommodation of newly integrated knowledge and skill. Accommodation is an end process in which the learner makes a conscious decision to modify existing ways of thinking and responding to satisfy new experiences and knowledge. Very often, accommodation results in significant qualitative changes in performance. An example of operations at this level would be the designers of networks that require interpretive techniques to assure varying levels of security. Capability to operate at this level is fostered through educational programs and processes.

The figure below shows an example of computer security content that is based on the learning continuum principle. Implicit in the example is the dynamic interrelation and interdependence of awareness, training and education activities.

Goal: Facilitate the increased use of password protection among employees.
Awareness Activities: Reminder stickers for keyboards
Training Activity: Computer Based Instruction on the use of passwords for agency specific machines
Educational Activity: A recognized COMPUSEC expert provides employees an opportunity to explore why passwords are used in general and evaluate the current agency protection techniques.

A true computer security learning program incorporates concepts and elements from each level and presents the employee/learner with a totally integrated succession of experiences. The next figure summarizes activities which many be found on each level of operation.

AWARENESS

Stimulation:	*Focus*:	*Attention*:	*Decisions*:
Security only colors	Change Locks	Bulletin Boards	Read Security Reg.
Security only music theme	Reminders	Flyers	Read Magazines
	Posters	Attend Lecture	

Assimilation:

Key ring with message	Short Demonstrations
Short Seminars	Video Tape Programs

TRAINING

Active Knowledge Seeker	*Long Term Memory*
Self Paced Course	Computer Based Instruction
OJT	Multi- Session Seminar

Conferences	
EDUCATION	
Internalization	*Accommodation*
Point Papers	Long Term Training
Study Groups	Research and Deliver Briefing

DAYS 4 AND 5 OF DACUM II

On days four and five the team began writing to fill in the newly designed Awareness Training and Education matrix.

The Results Review and Validation of DACUM I Results by New Group.

During the first day, the group reviewed the output from DACUM I. As noted earlier, consensus was reached about the definitions of Awareness, Training and Education. The team reviewed electronic versions of the awareness materials developed for FISSEA. The DACUM II team agreed that with modification[17] the materials would be useful. The National Information Assurance Training and Education Center agreed to function as a clearing house for these materials for FISSEA.

Review and Modification of Todd Model

The Todd model was reviewed by the group for consistency and applicability. It was agreed that the model was well conceived at the time; however, there were several issues that were overlooked. Since the Todd model concept was sound, the team decided to use it as a starting point for an expanded Federal AT&E program.

Todd Model NIST 500-172

The Todd model had been reviewed as part of DACUM I. The original model had five categories:

- Executives
- Program/Functional Managers
- IRM, Security, and Audit Personnel
- ADP Management, Operations and
- Programming Staff
- End Users

Todd Model as Revised by DACUM I

On the basis of a consensus reached during DACUM I, the granularity of categories was modified. The new categories were

- Executives
- Program Managers
- Functional Managers
- IRM
- Security and Audit
- ADP Management and Operations

---

17 To meet the requirements outlined by the DACUM 1.5 group, the new categories would be re-aligned.

- End Users[18]

The DACUM I team decided that the changes were appropriate for the awareness level activities. As the DACUM II team addressed the training activities, they decided that a category set that dealt with function performed rather than management level made more useful.[19]

Creation of New AT&E Matrix

After the team had identified the areas that needed change, they developed a new approach that combined the best of the Todd, McCumber, and NSTISSC models. After reviewing the Todd model, the team decided that the awareness materials and categories as modified by the DACUM 1.5[20] meeting would be adequate.

At the training level the team then decided to create categories based on functions. These categories were:

Manage Acquire Design and Implement Operate Use

The team realized that others may define new categories; therefore, they created a category called Other[21] to provide extensibility.

To provide transition from Awareness to Training, the team decided to prescribe a common knowledge base that would be expected for each of the functional categories. This element has been called Literacy and INFOSEC Basics. This is envisioned as a common course (above the Awareness level) across all Federal agencies. If an employee were to have had this background, he/she could be expected to enter any of the appropriate functional courses.

The team further recognized that 'Security Experts' had an entirely different set of expectations that could be described as Education. These individuals may enter through the functional category training path or may be dealt with here directly based on their experience. There has been discussion of having a DACUM III that would define the common body of knowledge required for this level. This activity would also be useful for professionialization efforts.

McCumber Model Applied To The New Matrix

The team also agreed to use the McCumber model as one of the components of the design of training materials. Before one can begin to develop an Awareness, Training and Education program, it is essential to establish the boundaries of the training requirements. The development of an AT&E focused on security of information addresses three dimensions that restructure the classical boundaries. The training model deals with information states, information characteristics and their associated security measures.

A. Information States	*B. Information Characteristics*	*C. Security Measures*
1. Transmission	1. Trust	1. Policy and Practice
2. Storage	2. Integrity	2. Technical
3. Processing	3. Confidentiality	3. Education and Training

18 Both DACUM I and DACUM II teams had problems with the End User category since it represents another view of the same individuals — everyone is an 'end user.'

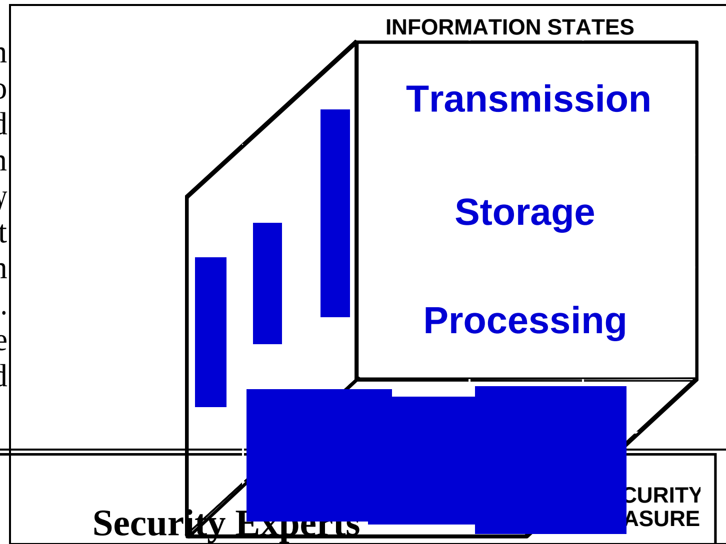
19 Note that the Todd model mixed functions and level in the Audience Category.

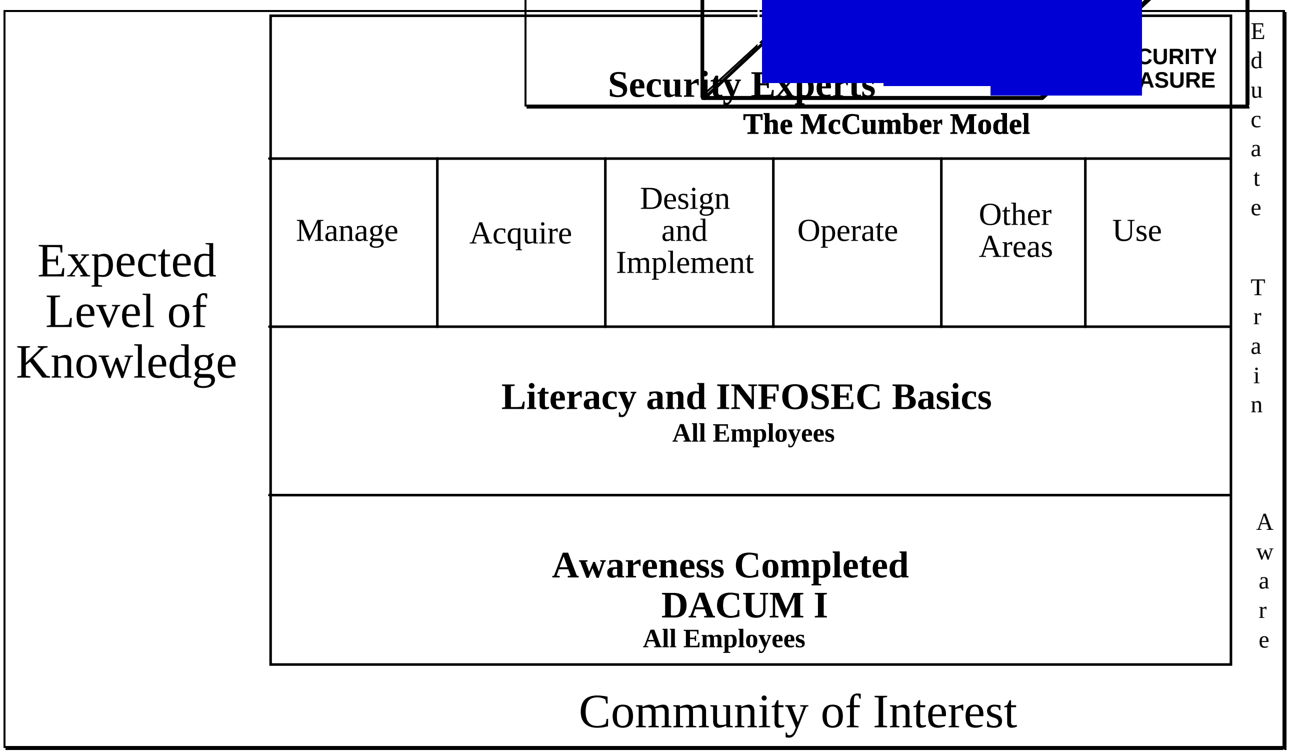
20 Held at Baltimore, May 1993.

21 The 'Other' category was often referred to as the *unknown god* . This is from the Classic Greek tradition of offering the first toast at the party to the unknown gods. The theory here was that if there were a god they had not yet identified, they would not insult him/her. Several others have been proposed and may be added in the future.

This approach to information security is represented in a model developed by John McCumber of the United States Air Force.[22]

This model has recently been extended by the author[23] to accommodate the Canadian Trusted Computer Product Evaluation Criteria[24] (CTCPEC) which explicitly split their criteria into two distinct groups: functionality and trust. Both of these can be addressed by AT&E. The following figure shows the relationship of the elements defined by DACUM II.





The basis of the DACUM II proposal is the awareness material developed at DACUM I. It provides minimum compliance with U.S. Code 5 CFR Part 930 subpart C.. After Federal

22 McCumber, John, "Information Systems Security: A Comprehensive Model", Proceedings of the 14th National Computer Security Conference, National Computer Security Center, p334, October 1991.

23 McCumber, John, "Application of the comprehensive INFOSEC Model: Mapping the Canadian Criteria for Systems Certification, Unpublished Manuscript, February 1993.

24 Canadian Systems Security Center, The Canadian Trusted Computer Product Evaluation Criteria, Draft Version 3.0e, April 1992.

employees have been made aware of their security responsibilities, they should take part in Literacy and INFOSEC Basics courses. This course could be developed as an agency independent training element. This should represent savings to the government.

The third component of the DACUM II model is Function Specific training. It is intended to be specific to agency needs.

The final component of the model is for security Experts. This is more of an Education rather than element. Both here and in the Function Specific Training, one would be expected to demonstrate performance and knowledge. It is expected that future work will be done to establish the knowledge and performance criteria in each category.

The DACUM II model is designed to be extensible by adding materials in the ‘Other Areas’ of the Function Specific Training. The authors and FISSEA expect suggestions for additions to this area.

4. DEVELOPMENT OF NEW MATERIALS.

Once the DACUM II model for the AT&E needs for Federal employees, it was necessary to determine what belonged in each level. The team used the products from day one and from DACUM I to create a list of performance based items for students. This list was then reviewed electronically and all items were moved to one or more of four different categories.

- Expert Knowledge (This is called ‘Above’ in the text)
- Function Specific Training
- Literacy/INFOSEC Basics
- Awareness or outside the domain of INFOSEC

Once the materials were distributed, the writing teams began the process of completing outlines.

To be Done

Establish Common Body of Knowledge for the security experts category. There was discussion that this might well be done by the National Information Assurance Training and Education Center and the Simplot Decision Support Center. This approach would allow the consistency among levels to be maintained.

Writing The Literacy—INFOSEC Basics

The team decided to create a small sub-group to write the Literacy/ INFOSEC Basics portion of this document. This three person team devoted to this task brought their INFOSEC knowledge and pedagogic skills to creating an instructional element to bridge the gap between Awareness and Training. The intent was to develop an outline for the pre-requisites for the training specific materials.

The following is the draft of the outline for the Literacy and INFOSEC Basics course.

Outline for Literacy—INFOSEC Basics

Purpose:

This instruction is intended to serve as a guideline for the development of curricula to provide the employee with the skill or ability to design, execute, or evaluate agency

INFOSEC procedures and practices. Elements of the 'Green Book'[25] may be used to develop materials for Literacy and INFOSEC Basics.

A. Information Technology

1. Telecommunications Basics
2. Computer Basics
3. Networks
4. Vocabulary

B. Information Systems Security Overview

A summary of the security disciplines and how they interrelate

C. INFOSEC Overview

Protection of information in information systems and access to resources

Physical Security

Construction Standards For Areas

Locks & Key Controls

Electronic Access Control Devices

Alarm Systems

Vaults And Secure Storage

Administrative Security

Categorization Of Information,

Confidentiality, Availability, Integrity, Sensitivity,

Classified V. Unclassified, Criticality

Communications Security

Brief Review Of The Basic Concepts Of Protection In Data Communication Systems And Networks From A Management Perspective.

Systems Objectives: Controlled Sharing Of Information And Resources.

Specific Needs: Privacy, Secrecy, Integrity And Availability.

Policies And Mechanisms.

Assets: Identification Of Valuable / Sensitive Data And Information.

Threats And Vulnerability.

The Interrelationship Of Communications Security And Network Security For Interconnected Elements:

Systems Connectivity

25 *Computer Security Modules,* Edited by Corey D. Schou, National Information Assurance Training and Education Center, Idaho State University, Pocatello, Idaho.

Public/Private Carriers

Relationship To Reliability And Dependability

Threats

Types Of Attacks/Failures

Passive Intrusion

Disclosure Of Message Contents

Traffic Analysis

Disclosure Of Data On Network Users

Active Intrusion

Modification Or Deletion Of Message Contents

Insertion Of Bogus Messages

Replay Or Reordering Of Messages

Viruses

Natural Disasters/Catastrophes/Sabotage

Human Errors

Fires, Floods, Brown-Outs.

- Locus Of Attack/Failure
- Terminals
- Hosts
- Front-Ends
- Gateways
- Links
- Switches (Includes Multiplexer, Intermediate Nodes)
- Interconnected Pc/Workstations (Includes LAN, Host-PC etc.)

Countermeasures

- Encryption
- Private-Key And Public-Key Systems - DES and RSA As Examples
- Key Distribution
- Link Level And End-To-End
- Authentication
- Node And User Authentication
- Passwords
- Message Authentication

Encryption-Based

Added Protection For Pc Authentication Date

Access Control

Access Control Mechanisms-Control Lists And Passwords

Administration

Contingency Planning

Approved Cryptographic Devices List

STU III use

FAX Connections & Controls

Emergency Plans (For Overseas Only)

Tradeoffs-Costs & Benefits

Accessibility Versus Secrecy

Personnel Security

Operational Security

Computer Security

Technical Security

Area Evaluations By Techies

Technical Countermeasures Missions

Testing Of Shielded Enclosures & Zoning

Vocabulary

C. Data Protection

Determination of Information Sensitivity

Access

Hardware & Software Controls

Back-up Procedures

Recovery Techniques

Data Encryption Uses

Disposition of Magnetic Media

Systemic Auditing

Evidence of Intrusion

(recognition that a system may have been intruded into. reporting and recognizing the event.)

D. Legislative & Ethical Considerations

National Authorities

Executive Orders, National Legislation, National Security Decisions Reference list, Appendix B, "Computer Security Basics," by Deborah Russell and G.T. Gangemi Sr., Published by O'Reilly & Associates, Inc., Sebastopol, Ca., December 1991, pages 277-288.

Director Central Intelligence, 1/16

Policy on Secure Voice (NCSC-8)

Policy for Safeguard & Control of COMSEC

NCSC-1 Requires agencies and departments to establish COMSEC material control systems. NCSC-1 Requires agencies and departments to establish COMSEC material control systems.

Policy of Use Of CRYPTO Material

NCSC-5 Provides guidance on the selection and protection of machine crypto systems for use in high risk environments. NCSC-5 Provides guidance on the selection and protection of machine crypto systems for use in hig

Industrial Security Program Concepts

National Telecommunications and INFO SYS SEC Policy

NTISSP 3

Communications Privacy Act

Fair Labor Standards Act

Omnibus Diplomatic Sec, Anti terrorism Act

Agency or Department Policies

Ethics

- Ethics in Government Act?
  - What reporting actions are required of the Agency
- Procurement Integrity Act
  - What reporting actions are required of the Agency
- Financial Managers Integrity Act
- Responsible Decision-Making
- Confidentiality & Privacy
- Piracy
- Fraud & Misuse
- Liability
- Copyright
- Trade Secrets
- Sabotage

Legal Considerations (Appropriate To Activity):

- Release Of Information From Agency Control
- "Private" Vs Work Use Of Computers
- Personal Use Of Government Equipment
- Intellectual Property Rights
- Duplication Of Licensed And Copyright Material
- Release Of Information To Contractors
- Release To Foreign Nationals
- Monitoring Of Employees
- Non-Disclosure Agreements
- Liability For Unauthorized Disclosure
- Computer Data As Evidence
- Federal Rules Of Evidence
- Privacy And Workforce Monitoring
- Contractual Agreements For Services
- Ownership Of Data
- Patent Secrecy Orders
- Protection Of Marked Proprietary
- Wiretapping
- Foreign Sales
- Foreign Govt. Information In Confidence
- Contract Award Protests
- Competition Sensitive Information
- Key Escrow Technology

E. How To Get Help

Organizational Activities That Provide Help:

- Computer Emergency Response
- Help Desk, Trouble Call, Or Systems Staff
- Courses, Conferences, Seminars
- Reference Materials & Updates
- Operating Procedures And Documentation
- Schedule Training
- Agency Specific On-Line Services

Fraud, Waste, And Abuse

On-Line Help Options

External Organizations And Sources That Provide Help:

Obtaining Federal Publications

Federal Computer Security Program Managers' Forum

National Institute Of Standards And Technology (NIST)

NIST Computer Security Bulletin Board

National Computer Security Center (NCSC)

DOCKMASTER

INTERNET Help

General Services Administration

Office Of Personnel Management

General Accounting Office

Office Of Management & Budget

Vendor Hotline Support

Agency Publications (Newsletters, Notices, Magazines)

Professional Associations

(E.G. Software Publishing Association,

Association Of Computer Machinery, (IEEE), etc.

Internal Organizational Personnel to Contact:

Information Systems Security Officer

Information/Procedural Security Officer

System Manager & Staff

Supervisor

Security Desk Officer

Communications Security Officer

F. Networks

Network navigation

Ability to move from one system to another in a network; communicate on a network

Vulnerabilities in distributed systems

G. General Knowledge

How To Login

How To Logout

Understanding Contingency Planning Concepts

Security In Relation To Productivity

Understanding Importance Of Identification And Authentication

Concept Of "Vulnerability" Vs. "Threat"

What Types Of Incidents Are Reportable

How To Report Incidents

Virus Protection

What User Activities Are Security Violations

Critical Characteristics Of Information

Writing The Training Specific Document

To facilitate the writing process of the training specific documents, each writing team was given an outline in the ETCORP/Paradigm writing tool. The following figure shows the contents of a typical outline.

1. Manage
2. Purpose
3. Definition Of Community
4. Definition Of Jobs
5. Define Terms And Concepts
6. Identify "Who Does What"
7. Outline Impact On Mission
8. Perform Following Skills In INFOSEC
9. Identify Risks
10. Identify Accreditation
11. Identify Personnel Security Needs
12. Identify Physical Security Needs
13. List Systems Documentation
14. Prepare Security-Related Plans
15. Identify Technological Issues
16. Identify Administrative Issues
17. Identify Sources Of Help
18. Identify Data Related Issues
19. Identify System Related Issues
20. Identify Database Issues
21. Identify Network Issues
22. Identify System Development Life Cycle Issues
23. Identify Operational Issues
24. Identify Training Issues
25. Identify Certification Issues
26. Identify Policy And Legal/Regulatory Issues
27. Identify Liability Issues
28. Identify Sound Computer Practices
29. Identify Labeling Issues
30. Identify Ethics/Conduct Issues
31. Identify Continuity Planning Issues
32. Identify Examples If Its Incidents
33. List Trade-Off/Cost-Benefit Issues
34. Outline States Of Information
35. Outline Characteristics Of Information
36. Identify Countermeasures
37. Parking Lot
38. Summary

The categories were selected from those developed during DACUM I. This was done to ensure that the awareness materials had a common thread with the training documents. The writing teams had complete control over their area and could change the outline if in their professional judgment it was best for the product. They were encouraged to use the power of the tool to share information within the document.

The following is the report from DACUM II. The contents have been edited for readability and spelling only. All deleted items referenced in the text were deleted by the original author. The only other items deleted were notes indicating the original author had not supplied a definition of the terms he/she was using.

I. Initial Question / Instructions

Complete the following outlines for your writing team. Use the On-line materials and writing from other sections as appropriate.

SAMPLE SLIDE SETS