MANAGEMENT OF INFORMATION TECHNOLOGY ACCESS CONTROLS

by

MICHAEL RAY POLLACK

B.S., University of Colorado, Colorado Springs, 1981

HQDA, MILPERCEN (DAPC-OPB-D

A thesis submitted to the

Faculty of the Graduate School of the

University of Colorado in partial fulfillment

of the requirements for the degree of

Master of Science

College of Business

1991

This thesis for the Master of Science degree by

Michael Ray Pollack

has been approved for the

College of Business

by

Carroll Frenzel

Carroll W. Frenzel

James C. Brancheau

Kenneth A. Kozar

Date 4/24/91

Pollack, Michael Ray (M.S., Business)

Management of Information Technology Access Controls

Thesis directed by Professor Carroll W. Frenzel

System access control directs, regulates, and coordinates the logical, physical, and administrative protection capabilities pertaining to interactions with an information system (IS). System access controls, a subset of information technology (IT) and general business controls, are IS security's critical first line of defense.

IT has traditionally progressed by increasing the speed and memory, and decreasing the size of centralized IS. However, recent movements toward distributed IS and the accompanying architectural changes present new management challenges, especially in the area of controlling system access.

Distributed IS magnifies potential control problems because it relies upon inherently less secure hardware and software, and increases potential system access points through local and telecommunication interconnection. However, the biggest threat to system access control is found within the organization's own workforce.

These issues motivated the development of an Access Control Management Model. The model details nine imperative management functions for system access control, supported by management tools. These iterative functions include adjusting management thinking, performing risk assessment, establishing access control objectives and a system access control plan, enforcing organization-wide access policies and procedures, choosing appropriate access control devices, continuously monitoring and periodically evaluating IT functions, and controlling system access revisions.

Information gathered from IT practitioners via questionnaires "face validated" the model. No changes were made to the order of the model, however, minor content changes were made. The following management tools were eliminated due to low respondent rankings: behavioral life cycle approach, organizational changes, employee security contracts, AI-intrusion detection, passive monitoring, and external audit. Risk assessment testing, asset ownership, and threat analysis were added as management tools. Staff exchange programs was rephrased as cross training.

Functional borders were blurred between performing risk assessment and establishing access control objectives, and between communicating access policies/procedures and selecting access control devices. The model's begin/end designator was also blurred because respondents felt there was little distinction between iterations of the model's functions.

The final access control management model comprehensively depicts how scholarly and corporate environments view the access control process and serves as a template for management action.

DEDICATION

I dedicate this thesis to my wife, Kathy, who supported and understood through the long hours it took to complete this work.

ACKNOWLEDGEMENTS

I would like to thank Dr. Carroll Frenzel for his guidance, experience, and patience as this work took form. Others who were instrumental in providing guidance, ideas, and survey participants were: Dr. James Brancheau, Dr. Kenneth Kozar, Dr. S. Mark Young, Dr. Sarah Bonner, Dr. R. Schaatke, Dr. James Nelson, Mr. Mike Galligan and Mr. Curtis Edfast (Association of Contingency Planners), Ms. Karen Holstein (EDP Auditors Association), Mr. Al Foster (Information Security Society of America), and Mr. Joseph Dailey (Data Processing Managers Association).

CONTENTS

CHAPTER

APPENDIX

FIGURES

Figure

CHAPTER I

INTRODUCTION

"Information is the most valuable asset of any organization."[1] Information Technology (IT) controls this valuable corporate data resourc.. The proliferation of IT to vital business functions has increased its importance to the firm. In performing these critical functions, information systems (IS) have become progressively more complex, and thus increasingly difficult to manage and protect.

Access control is basic to IS protection. Firms reduce the likelihood of damage to critical data resources, lower their overall vulnerability to internal and external threats, and identify or even prevent problems by maintaining adequate access control.

IT's progress can historically be measured in higher speed, expanding memory, and miniaturization of centralized (mainframe) IS. Over the years most firms have established reasonable levels of control over their mainframes. However, recent movements toward distributed IS present new management challenges, especially in the area of controlling system access.

This new distributed processing environment changes not only the architecture of the IS, but also expands the IT owner and user base dramatically. With distributed processing the IS Department no lcnger controls all corporate IT, and the IT Manager no longer controls every system and system interface. This makes traditional, technically-oriented IT management ineffective. If management does not evolve with this fundamental environment change, resulting security deficiencies will not be recognized and corrected in time to prevent the disastrous consequences of compromised security.

To ensure adequate management and consistent administration, it is critical that firms reassess access control in the broader context of distributed processing via a structured management process. IT management must be an integrated effort based on an overall view of system security goals and strategies. Management must develop concepts, guidelines, and rules for managers, technicians, and users to follow. A common vision of security must exist if individual business functions and the firm as a whole are to safely use IT to common advantage. This effort starts with system access control.

Research Goals

Four goals guided this research. The first was to determine the management functions and supporting tools critical to the success of IT management and overall system access control. A second goal was to use these functions and tools to construct an access control management model. A third was to "face validate" the model with IT practitioners, determining the extent to which they accept the model's concepts. The final goal was to integrate these findings with the scholarly model to create a comprehensive, realistic model for IT access control management.

Methodology

Initial research included a thorough review of scholarly books, theses, current periodicals, industry journals, and IT management case studies. This was used for initial background information and for constructing the initial access control management model. Questionnaires were used to gather corporate IT practitioner responses and validate the access control management model.

Thesis Organization

The thesis begins with a discussion of general business, IT, and system access controls in Chapter Two. Chapter Three identifies a variety of security threats with which IT management is faced. Chapter Four examines traditional security programs currently used by many firms and looks at access control factors in a distributed processing environment. Chapter Five introduces the access control management model based on initial research. Chapter Six discusses research methodology, including selection of participants and conduct of the research. Chapter Seven includes a summary discussion of questionnaire results. Chapter Eight merges information from questionnaires with the original access control management model to form a final model. Chapter Nine summarizes final conclusions from all research and discusses future research directions.

NOTES - CHAPTER I

1. Hussein Bidgoli and Reza Azarmsa, "Computer Security: New Managerial Concern for the 1980's and Beyond", Journal of Systems Management, (October 1989): 22.

CHAPTER II

SYSTEM ACCESS CONTROL

System access control is a subset of the general business controls which all firms employ in varying degrees. Therefore, it will help to discuss the macro level of general business controls before exploring system access controls in detail.

What is Control?

Control in an organization is likened to the task of steering an automobile. A driver's control is maintained through a continuous process of checking the progress of the vehicle against the planned route and standards of conduct on the road. Any violation must be corrected immediately in order to continue on the appointed course. Uncorrected violations reduce the efficiency of the driving at least, and could have potential for disastrous results.

Management performs the "steering" in organizations. It has the task of "measuring and checking of results against plans and standards and the introduction of corrective action with a minimum of delay once deviation is observed."[1]

Control is formally defined as "the application of policies and procedures for directing, regulating and coordinating production, administration and other business activities in a way to achieve the objectives of the enterprise."[2]

In simpler terms, control is the state of "knowing the details of the significant activities taking place within the organization." This knowledge includes the What, When, Where, Why, How, and Who for important business functions.[3]

Types of Control

Control takes three forms.[4] First, there is strategic planning. This is the long-term management vision that guides and unifies organization actions; it is the "road map" that the management "steering process" follows. Management control, the second form, is the process of influencing organization members to implement organizational strategies devised in strategic planning. Finally, there is task control which addresses more immediate, lower-level supporting functions using monitoring and feedback techniques to compare performance to goals. Typical task controls for an IT organization are summarized in Figure 2.1.[5] All three control forms are needed for a total control environment.

Management Control Systems

The three control forms are implemented through management control systems. Effective management is widely recognized as a combination of four basic elements: planning, coordinating, directing, and controlling. These elements are the basis for the principles used in management control systems. These systems attempt to allocate human, physical and technology

* **Operational Procedures**

* **Compliance with Procedures**

* **Reconciliation**

* **Timeliness**

* **Management Records**

* **Management Involvement**

* **Follow-Up's**

* **Automated Systems**

* **File Controls**

* **Separation of Duties**

* **Security (physical)**

* **Control Across Functional Lines**

* **Job Understanding**

Figure 2.1: Fundamental Business Task Controls
Source: IBM Business Control Manual ASCH 12/1

resources to ensure organizational goals are reached. A management control system is concerned primarily with the coordination, information processing, and resource allocation aspects of management.[6]

Management Control Systems consist of two elements: a structure (what the system is) and a process (what the system does). The semi-permanent structure element includes the organization, degree of freedom given to management, the communication flows within the organization, and the responsibilities of the various organizational units. The more dynamic process consists of management decisions that plan for and control resources, evaluate performance, and review feedback.[7]

Business Functions

The environment in which managers must apply management control systems consists of various business functional areas. These functions are constantly changing in importance and structure.

In 1968, Boyce broke the organizational control environment into five general business areas: objectives, production, marketing, financial management, and personnel management.[8] Objectives concern the organization's top management control over the other four business activities. Production factors include labor, materials, machines, and the resulting output. Marketing is comprised of sales, distribution, and warehousing functions to make products available to business clients. Financial management systems control overhead, expenses, and labor and material costs. Finally, wages, leave, promotion, hiring, and firing are concerns of personnel management.

In 1967, Cashin defined business control areas in a slightly broader way. Cashin's four control areas consist of general management, marketing, manufacturing, and finance.[9] The personnel function described by Boyce is absorbed into the general management function.

These business areas and controls are not as exclusive as they may first seem. For example, a firm's marketing department devises its own internal strategies and plans (which of course should tie in with those of the organization), controls its own quality of output, manages finances per its budget, and approves personnel actions for its employees.

Boyce and Cashin both failed to address IT as a critical aspect of business controls. This can be attributed to the period of their writings. IT controls have become increasingly important in the last twenty years, not only to the IT organization, but to the firm as a whole.

Frenzel addressed the growing firm-wide importance of IT controls through three trends.[10] First, IT control is essential to the firm because other organizations within the firm now rely on IT for their control processes. Second, the introduction of new technology creates a need for more control, and IT is the major contributor to advancements in the firm today. Finally, executives are becoming more "computer literate" and realize what IT can do for them. They put more pressure on the IT organization to provide leadership in business functions and their control.

For these reasons, IT control now deserves a place with the other general business control areas. In the following model which describes overall business controls, IT control is included as one of six functional area management control systems (See Figure 2.2). This model is not meant to exhaust all possible organizational controls, but is a graphical attempt to place IT and access controls in the overall realm of general business controls.

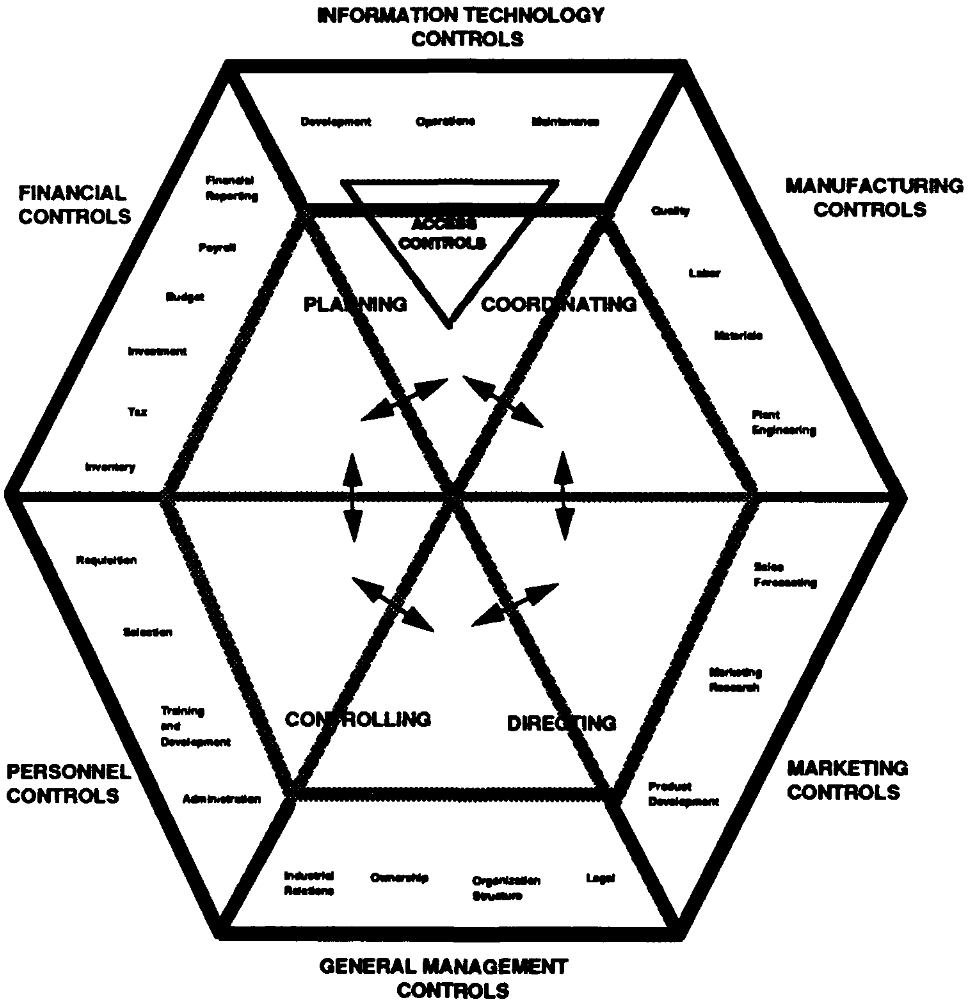


Figure 2.2: Management Control System Model

In the Management Control System Model, each functional area management control system is broken into two parts: that which includes controls unique to the function (the outer band), and the other containing controls used by more than one functional area (the inner band). The arrows within the inner band signify the sharing of controls between functional areas. The permeable division between unique and common controls suggests the possibility of some unique controls, such as access controls, becoming more common within the organization over time. The four basic management elements are included in the common controls of all functional areas.

Information Technology and Access Controls

Distinguishing IT controls is difficult because the IT function within most firms is no different than the earlier marketing example. General business controls and IT controls are not mutually exclusive. Common general business controls are used to manage IT within the IT function, and because IT is now found throughout the firm, there are many IT controls which are common to other business functional areas. Management of the IT function is based on ensuring control in all six areas depicted in Figure 2.2. Regarding general management controls, for example, management must ensure separation of application development, maintenance, and daily operations functions within the IT department by designating separate responsibilities for these activities.

System Access Controls

System access controls are simply a subset of general business and IT controls that apply specifically to system access. To define system access control it is helpful to first define each piece of the phrase. A system is defined as "an organization or network for the collection and distribution of information, news, or entertainment."[11] The definition of access is "the permission, liberty or ability to enter, approach, communicate with or pass to or from."[12]

Combining these with the previous definition of control formally defines what system access control is: the application of policies and procedures for directing, regulating and coordinating the ability to enter or communicate with a network for the collection and distribution of information.

Lobel describes computer access control as "the combination of logical, physical, and administrative protection capabilities that are associated with a computer system or information network."[13]

The model implies that IT controls are a critical part of all organizational controls. As IT becomes more engrained in every aspect of the firm, it supplies a greater impetus for competitive advantage. Many critical business functions and the controls that guide them are becoming part of the overall corporate IS. This trend is predicted to continue as IT proliferates throughout the firm. "As information systems become more critical to the strategic mission of organizations, general system controls become increasingly important."[14]

If access control isn't yet central to overall business controls, it certainly is the heart of IT controls. This point is graphically detailed by Nota's Data Manipulation Process (see Figure 2.3).[15] Here, environmental controls (physical access) and PC access (logical access) are the first two lines of defense against threats. Fortifications in these areas will prevent unauthorized data manipulation.

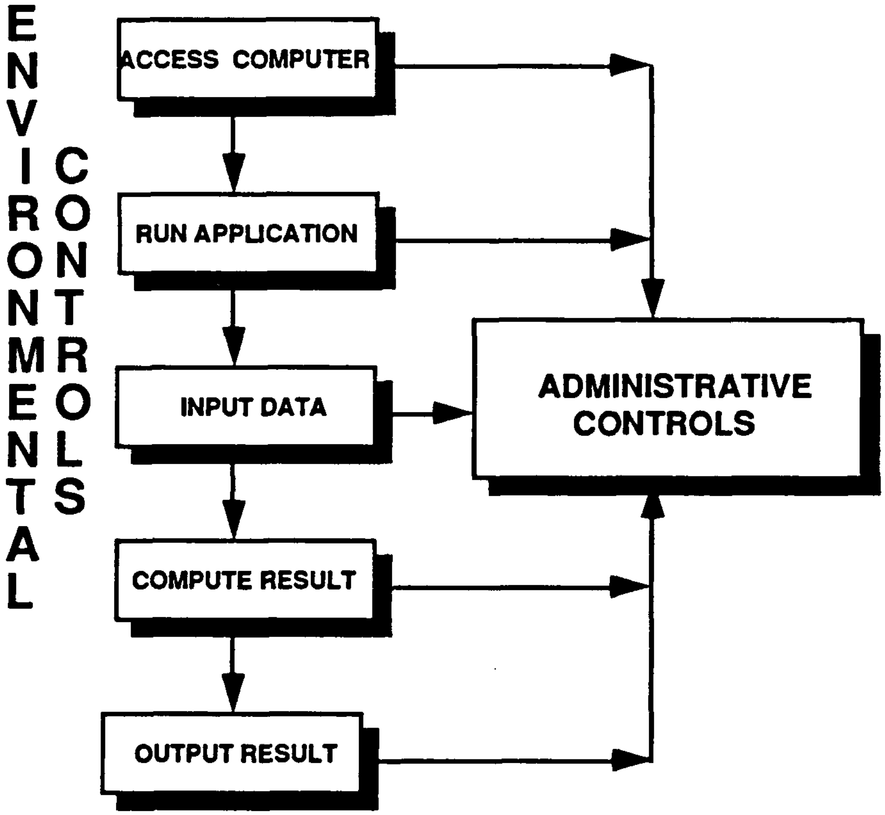


Figure 2.3: The Data Manipulation Process
Source: Peter Nota, "Data Manipulation in a Secure Environment", Accountancy, (June 1989): 142.

"Access control protection is basic to a workable security system. If unauthorized personnel cannot gain entry to the computer facilities, then the chance for harm is considerably reduced."[16]

Effective access control goes a long way toward effective overall IS security that is becoming increasingly important for corporate control and survival.

NOTES - CHAPTER II

1. R.O. Boyce, Integrated Managerial Controls: A Visual Approach Through Integrated Management Information Systems, (New York: American Elsevier Publishing Company, ¹968), 8.

2. Webster's Third New International Dictionary, Unabridged. G&C Merriam Company, 1976, 496.

3. Carroll W. Frenzel, The Management of Information Technology, (Boulder, CO: N.P. 1990), 480.

4. Robert N. Anthony, John Dearden and Norton M. Bedford, Management Control Systems, (Homewood, IL: Richard D. Irwin Incorporated, 1989), 11.

5. IBM Business Controls Manual ASCH 12/1

6. Joseph A. Maciariello, Management Controls Systems, (Englewood Cliffs, NJ: Prentice-Hall Incorporated, 1984), 2.

7. Ibid, 3.

8. Boyce, 6.

9. James A. Cashin, Management Controls, (Hempstead, NY: Hofstra University Yearbook of Business, Series 4, Volume 2, 1967), 4.

10. Frenzel, 481.

11. Webster's, 2322.

12. Ibid, 11.

13. Jerome Lobel, Foiling the System Breakers (New York: McGraw-Hill Book Company, 1986, 11.

14. Keith Burgess, Per O. Flaatten, Donald J. McCubbrey, P. Declan O'Riordan, Foundations of Business Systems (Chicago: The Dryden Press, 1989), 518.

15. Peter Nota, "Data Manipulation in a Secure Environment", Accountancy (June 1989): 142.

16. John G. Burch and Joseph L. Sardinas, Computer Control and Audit: A Total Systems Approach (Santa Barbara: Wiley and Sons, 1978), 217.

CHAPTER III

SECURITY CONCERNS

Before determining what management can do to promote effective access control it is necessary to identify the threats to access security. When many people think about computer security threats they picture perhaps a young "War Games" hacker trying to play mischievous tricks with Department of Defense computers, or maybe a student releasing computer viruses to disable computer networks nationwide.

While these are legitimate threats they are certainly not the only, nor the most common ones. These images stand out because they have gained the most publicity in recent years. However, corporate America faces more frequent and equally dangerous daily threats.

> Each day, computers and the networks that connect them transmit close to $1 trillion among financial institutions, and corporations transfer critical information often worth much more. Each of these transactions is vulnerable to tampering. Given the heavy corporate reliance on computers and networks, studies indicate that tamperings and the resulting downtime cost the private sector $3 billion to $5 billion annually.[1]

Defining Threats

Threats fall into one of three categories: man-made errors or omissions, man-made intentional acts, or disasters caused by nature.[2] Because access control is not commonly affected by natural disasters and the scope of this thesis does not include contingency planning, I will concentrate on the human-related threats.

Types of Threats

Human-related threats come in four basic forms: Fraud, sabotage, disclosure and error.[3]

Fraud. Fraud appears as embezzlement, and simple theft of programs or computer time.[4]

Embezzlement by computer involves the stealing of funds. In 1983, the Federal Bureau of Investigation (FBI) investigated 7,811 cases of this type. The total money involved was approximately $282 million. This is more than seven times the amount reported stolen from actual bank robberies during the same year.[5]

Although fraud makes up a major portion of the estimated total security threat (sixty-four percent), most of it is not reported.[6] In the United Kingdom, up to eighty percent of estimated computer fraud cases go unreported.[7] FBI statistics indicate only one in every 800 computer crimes is reported.[8] In the United States, where the average embezzlement case involves theft of $500,000, only ten percent of cases reported result in any type of conviction.[9] The conveyed message is that computer crime pays big, with few consequences.

Other types of theft are seemingly less harmful. Employees often make unauthorized copies of software programs for use at home. Although this is stealing, it is mostly considered innocent "borrowing" by the thieves. Even less tangible is theft of computer services. Use of a firm's computer by employees or by outside hackers does not involve a measurable physical loss and is therefore difficult for firms to quantify. The intangible nature of computer resource theft tends to legitimize it in the eyes of the thief. However, firms lose considerable amounts of computer resources to this theft of computer time.

Sabotage. Sabotage does not involve the direct theft of money but has equal or possibly greater effects on the firm involved. Sabotage is harm directed against a computer facility with the intention of disabling it, damaging its software, or altering its data stores. Sabotage comprises an estimated twenty-eight percent of the computer threat.[10] The most likely source of sabotage is an employee of the firm. The motivation is usually a past disciplinary action, failure to promote, or perhaps even job termination.

Such was the case in the widely-publicized 1985 incident involving Donald Gene Burleson, formerly of USPA & IRA security traders. Shortly after his termination Burleson accessed corporate computers, planting a program that eventually wiped out over 168,000 company records.[11]

Outsiders can also sabotage IS, often by very simple means. For example, the system Dr. Jerry Falwell's ministry uses for collecting donations was disabled by a man who set his home modem to auto-redial the ministry's access number. This effectively blocked the collection of donations estimated in the millions of dollars.[12]

This example points out another significant cost of computer insecurity: system nonavailability. An airline the size of American Airlines "could lose as much as $34,000 in booking fees for each hour that its reservation system is down".[13] Infonetics, a market research firm, reports downtime costs businesses up to five percent of their annual revenues when lost business, administrative costs, troubleshooting expenses, lost productivity, and support costs are included.[14]

Disclosure. Disclosure is often more innocent than either fraud or sabotage, but no less harmful. Disclosure refers to the compromise of sensitive or unique corporate data. Again, the source is typically an employee of the firm. This employee may or may not be aware that disclosure of the information could result in loss of competitive advantage, loss of customers (in the case of privacy issues), loss of revenue, or embarrassment for the firm. A well-known disclosure incident involved the members of NBC's Today Show. Host Bryant Gumbel's personal memos containing derogatory remarks about other cast members were stolen from his personal computer and then released to the press. The show suffered great embarrassment as a result.[15]

Error. Error differs from the previous three threats in that it is accidental. For example, files can be erroneously deleted by an improperly trained employee, or incorrectly entered data can corrupt the integrity of system data. The effects of errors vary in severity depending on the type and amount of data involved. Although this threat is not deliberate (deliberate errors fall into the category of sabotage), the loss is just as real.

Categorizing Threats

These human-related threats can be partitioned by both source and intent. Threat sources include those inside the firm (company employees) and outside the firm (hackers, for example). Intent can be either passive or active. Passive intent includes activities such as snooping through files, reading electronic mail or facsimile transmissions, penetrating systems access security for fun (hacking), or simply making errors. Active intent includes malicious destruction, manipulation, misuse, denial of use, or deliberate disclosure of corporate information.

Figure 3.1 portrays this threat categorization, including examples of each threat category. Examples such as disclosure appear in more than one category. An employee can either intentionally disclose corporate information or unintentionally leave sensitive information on the monitor screen, allowing unauthorized persons to see the information. In the first case the disclosure is active; it is passive in the latter.

Corporate information can also be disclosed by outsiders. Thus, disclosure appears in three partitions of Figure 3.1.

The Main Threat

Where do most threats originate? "Experts agree that the number one threat, which accounts for at least eighty percent of security breaches, is internal."[16] "The National Center for Computer Crime Data (NCCCD), based in Los Angeles, reports that computer-related crimes were most often committed by programmers, students, and data entry operators."[17] Don Parker, senior management consultant in the information and computer security program at the Stanford Research Institute, also concludes employees are the biggest security problem. His research included over 1,700 computer crime cases worldwide.[18] The remaining threats come from other sources including hackers, extremists with political motivations, and career criminals who learn computing solely to commit crimes. All are threats, however, Mr. Parker concludes that employees deserve the most management attention.[19]

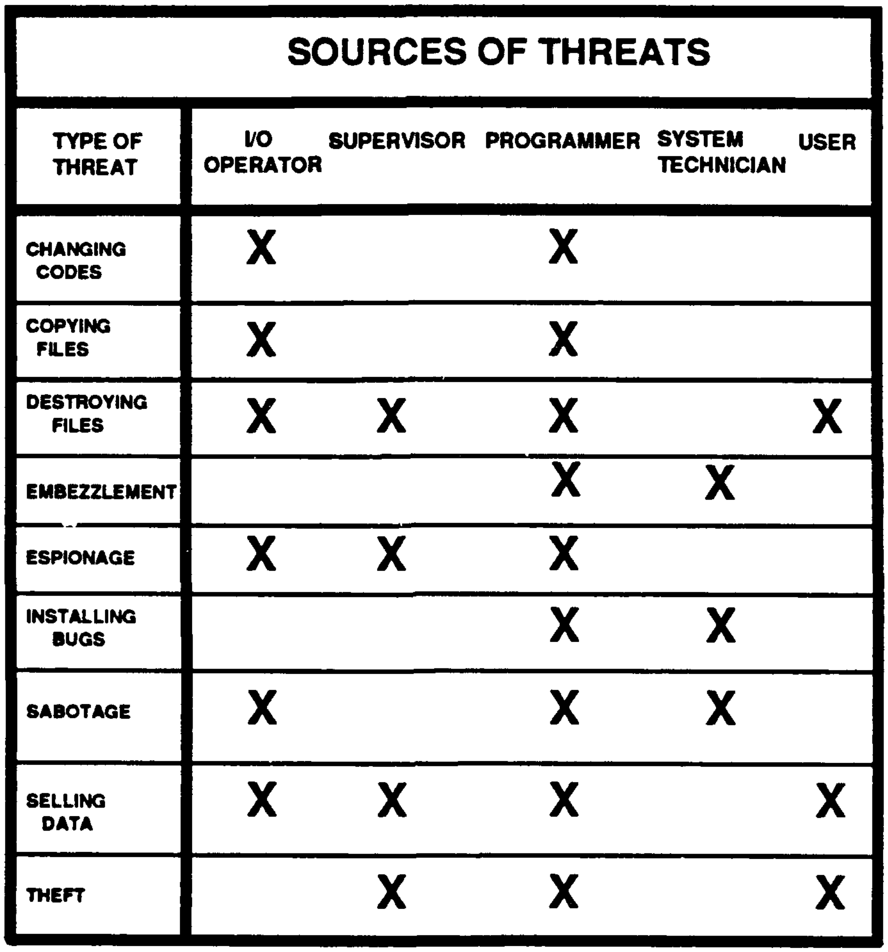
	PASSIVE	ACTIVE
INTERNAL (Employees)	READING E-MAIL ERROR SNOOPING DISCLOSURE	FRAUD EMBEZZLEMENT THEFT OF SOFTWARE UNUATHORIZED USE SABOTAGE DENIAL OF USE DESTRUCTION MANIPULATION DISCLOSURE
EXTERNAL (Hackers, Extremists, Criminals)	READING E-MAIL SNOOPING HACKING	FRAUD COMPUTER VIRUS UNUATHORIZED USE SABOTAGE DENIAL OF USE DISCLOSURE

Figure 3.1: Access Security Threats
Source: Personal Conversation with Carroll W. Frenzel

The extent to which internal personnel pose a threat depends greatly on the amount of access they are granted. The Journal of Systems Management developed such a depiction of threats and their sources in 1989 (Figure 3.2).[20] Programmers and I/O Operators have the most threat potential because of their generally greater access privileges. This figure introduces threats not mentioned in Figure 3.1 or in the previous text, however, these and all threats can be categorized (as fraud, sabotage, disclosure, or error) and partitioned by source and intent. For example, the threat of changing codes is active sabotage that arises from both internal and external sources.

The Future

Threats to information security are likely to increase in the future due to three trends. First is the growing computer literacy of the general public. More people gain the knowledge necessary to interact destructively with computers each year. Second is the lack of follow-up by corporations. For example, in 1986, only seventy-five cases of computer crime were filed in prosecutors' offices in thirty-eight states.[21] Most firms either handle matters internally, or fail to handle them at all. The final trend is distributed processing, the topic of Chapter Four.



	SOURCES OF THREATS				
TYPE OF THREAT	I/O OPERATOR	SUPERVISOR	PROGRAMMER	SYSTEM TECHNICIAN	USER
CHANGING CODES	X		X		
COPYING FILES	X		X		
DESTROYING FILES	X	X	X		X
EMBEZZLEMENT			X	X	
ESPIONAGE	X	X	X		
INSTALLING BUGS			X	X	
SABOTAGE	X		X	X	
SELLING DATA	X	X	X		X
THEFT		X	X		X

Figure 3.2: Internal Computer Threats and Vulnerability. Adapted from Hussein Bidgoli and Reza Azarmsa, "Computer Security: New Managerial Concern for the 1980's and Beyond", Journal of Systems Management (October 1989): 23.

NOTES - CHAPTER III

1. Melvin Schwartz, "Computer Security: Planning to Protect Corporate Assets", The Journal of Business Strategy (January-February 1990): 38.

2. Donn B. Parker, Computer Security Management (Reston: Reston Publishing company Incorporated, 1981), 43.

3. Grant Findlay, "Data Security: Reducing the Risks", The Accountant's Magazine (June 1987): 57.

4. Jerome Gilbert, "Computer Crime: Detection and Prevention", Journal of Property Management (March-April 1989): 64.

5. Ibid, 64.

6. Hussein Bidgoli and Reza Azarmsa, "Computer Security: New Managerial Concern for the 1980's and Beyond", Journal of Systems Management, (October 1989): 21.

7. Findlay, 57.

8. Kevin Wilson, "Coping With Computer Crime", Records Management Quarterly (July 1989): 56.

9. Findlay, 57.

10. Bidgoli and Azarmsa, 21.

11. Katherine M. Hafner, "Is Your Computer Secure?", Business Week (August 1, 1988): 64.

12. Wilson, 56.

13. Schwartz, 39.

14. Ibid.

15. Michael Alexander, "Holding Your End Users Accountable", Computerworld (May 1, 1989): 39.

16. Hafner, 64.

17. Bidgoli and Azarmsa, 21.

18. William K. Makley, "Computer Security's Worst Enemy: Management Apathy", The Office (March 1987): 115.

19. Ibid.

20. Bidgoli and Azarmsa, 23.

21. Makley, 115.

CHAPTER IV

SECURITY IN A DISTRIBUTED PROCESSING ENVIRONMENT

The Tradition

"Unfortunately, the only way to truly secure a computer is to lock it away in a 'glass room' and not give it a communication line."[1] Fortunately for early IS managers, this is the way it was. Computer security programs in the traditional centralized processing environment consisted of restricting mainframe access to the few technicians that had the expertise to use it.

A simple system of physical access control via badges or combination locks was enough to limit entrance to the data processing area. The only terminals hooked to the mainframe were located in the same secure room and were again used only by a handful of technical experts. These "dumb" terminals had no internal memory or processing capability and were used only to interact directly with the mainframe.[2] Because the resources were in a fairly limited area the cost of physically securing them was nominal.

The tasks performed by the mainframe were also traditionally simpler. Computers' usefulness began by automating repetitive activities such as payroll or accounting functions. Application programs performing these functions were independent of each other, affecting a single activity. Managers could easily track what the program did by monitoring that one function. Auditing of automated systems was easily done because they closely resembled the old manual systems.

Average employee involvement was restricted to specifying needs for system development. The computer was a never-seen monster that took in data and spit out reports. If the reports kept coming everything was fine; if the reports stopped something was amiss. Non-technical managers didn't have (and didn't want to have) a clue as to what the problem was or how to fix it. This, after all, was the responsibility of the "computer guys".

The Change

The nature of computer technology is change. Until recently, most of the change could be measured in speed and size of the hardware, or sophistication of the software used. The one constant in all this change was the architectural concept of a central mainframe controlling either dumb terminals or possibly linked to limited function terminals.

The distributed processing trend now gaining momentum is changing the basic architecture of IS. The power of the personal computer/microcomputer (PC) and the parallel advances in telecommunication have created an environment where a network of smaller computers linked to specialized minicomputer servers can outperform the mainframe configuration.[3]

The advantages of this architecture are numerous.[4] First, a specialized server can perform a particular task for the network and do it better than a mainframe, which must perform multiple tasks. Second, the modularity of such a network makes it flexible; able to adapt to the ever-changing needs of business. This modularity also reduces the cost of maintenance and upgrading the system. System upgrades involve changing smaller, less costly components rather than changing mainframes or performing extensive reprogramming. Because of the advanced programming tools provided with PCs, the cost of writing programs on PCs is estimated to be one-tenth that of programming on mainframes. Third, the cost of microprocessor-based networks is now lower than that of mainframe-based systems. Finally, the network system provides the user access to all network information while giving the illusion that everything is happening on the user network node.

The shift to networked systems is already occurring at an estimated rate of thirty-percent annually. The 1989 network server market of $3.2 billion is expected to reach $117 billion by 1994.[5] The only factors that seem to have a chance at slowing this movement down are existing mainframe investments and possible network hardware incompatibilities.

The proliferation of computers to all aspects of business has increased firms' reliance upon them. Computers are now responsible for critical business functions requiring one hundred percent availability. Information has become the most critical asset to firms. More than half of all employees now use computers as part of their work. The ease of use and expanded functionality of PC applications has lured (and sometimes forced) most employees and managers into becoming computer literate.

The Effect on Security

The trend is clear: future businesses will run on microprocessor-based networks. In terms of access security this makes more data available to users who will be able to share it more easily with other users.[6] This means security headaches if management does not adequately plan for this change and implement measures to counteract the demands for increased security.

A comparison of mainframe and distributed processing environments is shown in Figure 4.1.[7] This depicts the number of people having the potential to harm a system, the type of threat (fraud or sabotage), and the relative skill level needed. In the distributed processing environment both the employee and outsider threat increases dramatically. This increase can be attributed to several factors.

The Factors

The design of the PC is not secure, having been originally designed for an uncontrolled environment as a utility. PC operating systems are not designed to control access the way mainframe operating systems are. PC access control software is available, but at an additional cost many users are not willing to pay.[8]

Second, network systems increase potential system access points. Every terminal or node represents another critical gateway to the network and its data. With network links, these terminals are spread over a wider area making control even more difficult. "The multiplicity of interconnections means that managers have a harder time identifying the potential point of security breakdowns."[9]

This interconnection problem magnifies when network systems are linked via telecommunications to other local networked systems, and sharing of programs and data within the network also occurs between networks. In this context the scope of system security quickly becomes global.

Fourth, networked PCs also have the capability of resident data storage. Many times, work done on PCs is stored on their hard drives without being entered into the network. This data may be as confidential as anything

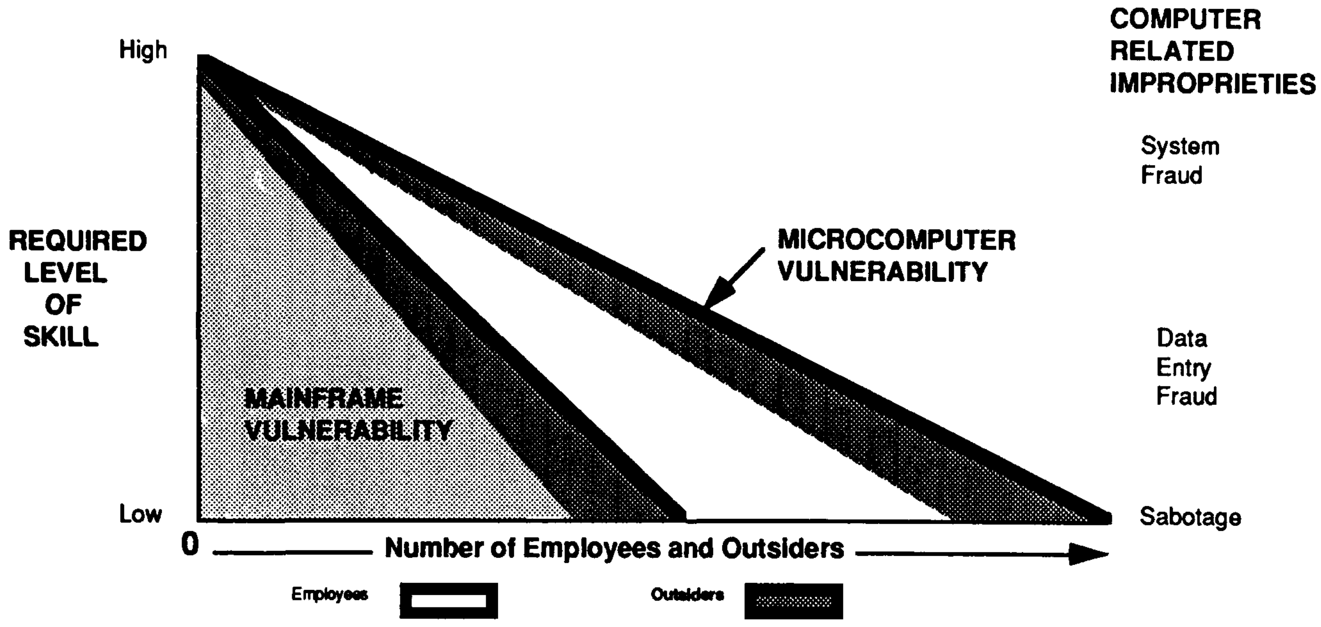


Figure 4.1: Vulnerability in the Micro-Pervasive Environment.
Source: Jonathan D. Harris and Gerald
M. Ward, Managing Computer Risk: A Guide For The Policymaker, (New York: John Wiley and Sons, 1986), 32.

on the network, resulting in a multitude of uncontrolled data stores waiting to be accessed. Access control for PC data stores is minimal compared to that of traditional mainframe systems. The access control on an IBM PS/2 is a classic example of this. "If you forget the password, all you have to do is turn the battery off for twenty minutes and turn it back on. Then anyone can access the system. It tells you how to do it in the manual."[10]

Finally, the increased integration to be provided by the Integrated Services Digital Network (ISDN) will further increase remote access capabilities.

> Currently, economic and technical constraints on terminal access proliferation serve as a default, surrogate means to reduce (...) system intrusion risks. Under ISDN, these restraints will be seriously eroded.[11]

The new connectivity and standardization provided by ISDN will allow access by almost any type of hardware. As corporate operations become more highly automated the effects of errors, omissions, or intentional acts spread through the firm very rapidly causing widespread damage.[12] This issue of control increases in importance as IT spreads.

The Results

The effect of distributed processing becomes clear if one thinks what would occur if the same controls were applied to the existing mainframe environment. First, remove the secured room, take away the sophisticated operating system, and make one person responsible for all activities (effectively negating any separation of duties). Next, try to use this system to accomplish tasks critical to business survival without possible compromise. This impossible task is much the same as what some businesses are trying to do with their new distributed IS.[13]

The PC revolution has left most firms with an overall IS comprised of several sub-system types. First, there may be stand-alone PC systems. There may also be PCs directly linked to a host computer. In this case the satellite terminals have no communications capabilities. Finally, there may be communication-capable PC or work station networked systems. Any combination of these now exist in the corporate world.[14]

The overall system type directly affects the access control necessary to protect resident data and programs. Stand-alone systems force the focus to physical access. Although not usually highly technical, measures such as locks or surveillance systems are expensive to implement for every stand-alone system compared to the single system which was adequate to protect yesterday's centralized mainframe. Logical protection must be afforded to linked systems whether communication facilities are available or not. Even more stringent logical and communication security measures are necessary for host and satellite terminals alike if outside communications gateways exist.[15]

The problem with all of these access controls is that employee cooperation is necessary to make them work.

> "They [management] know as well as anyone that an employee who chooses not to protect or conceal his or her personal password to a sensitive file is capable of compromising almost any technical system security program or technical protection mechanism. The point is, of course, that employee confidence and trust cannot be taken for granted."[16]

With this in mind, it is unfortunate that the attitude toward security of networks is generally lax.

> "Today's desktop computers have almost as much power and memory as many corporate computer center of only a decade ago. But whereas the "old" computer center was likely to be the most secure environment in the corporation, administered by specialists in white lab coats in an air-conditioned sanctum, today's networked

> desktop workstation is often viewed as just another fixture in the typical office."[17]

To make matters worse, users concern themselves primarily with the utility of the IS; security is a minor issue.[18] Combatting this kind of attitude is certainly a tough challenge, but at least some believe it is a challenge that management can rise to.

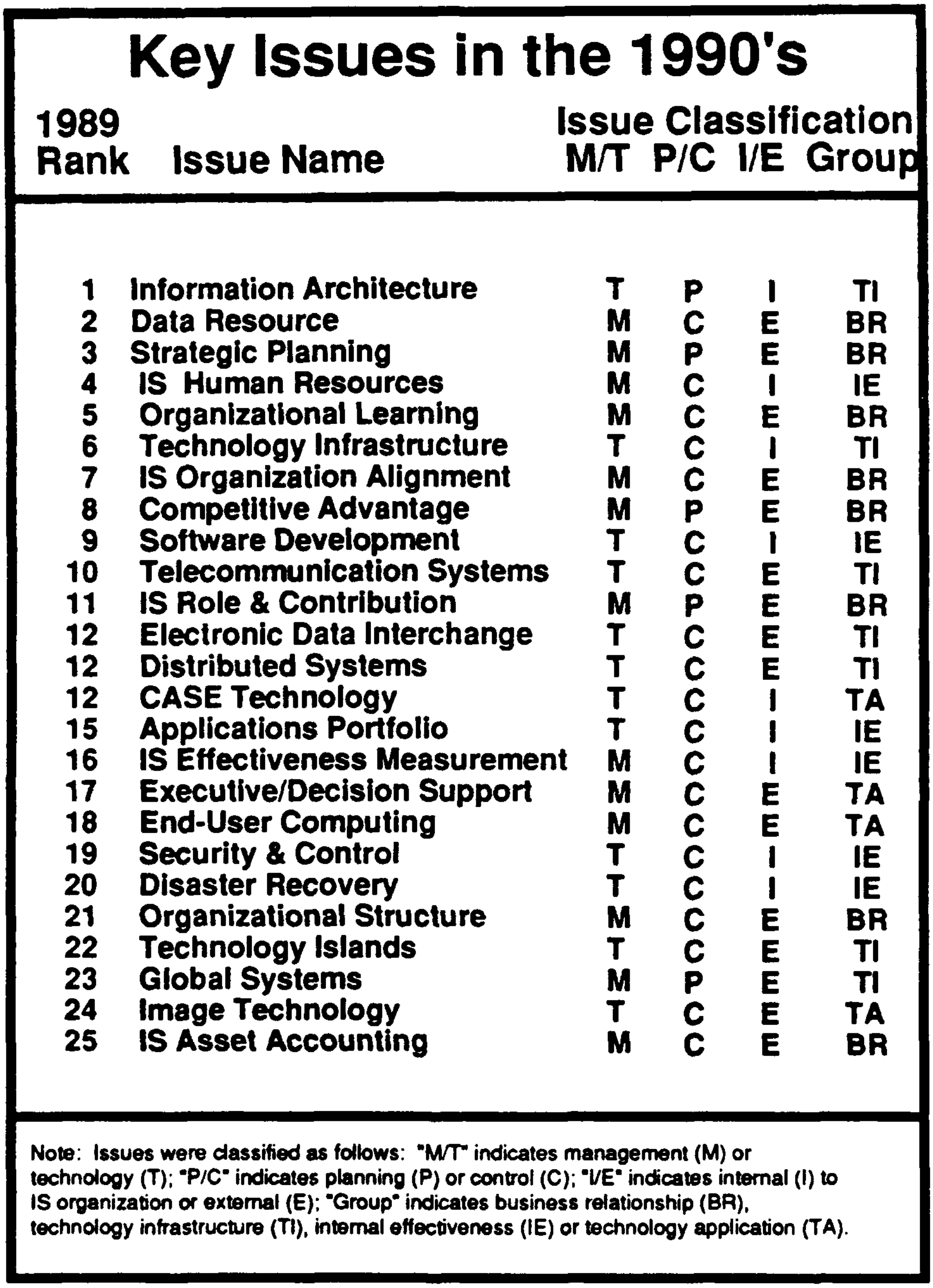
> "Those who are worried by all this talk of emerging security issues might find comfort in knowing that the security experts say the most effective solutions still rest with the way management handles technology, not just with the technology itself".[19]

A Problem?

Is management aware of this revolution and the resulting security problems? In a 1990 University of Colorado Working Paper survey of key issues for the 1990's (see Figure 4.2), senior IS executives included four related issues in the top twenty. Two new issues, technology infrastructure and distributed systems, were ranked sixth and twelfth respectively. End user computing held the eighteenth position while security and control was ranked nineteenth in importance.[20] This study provides evidence that IS managers indeed recognize the trend toward networked systems and are also concerned with security and control of these new systems.

However, a disconcerting portion of the survey is that security and control was classified as primarily a technology rather than a management issue by the survey authors.[21] This raises the question of whether some business professionals and academics may not recognize people as the main security threat, nor management's inherent responsibility to control that threat.

The importance of distributed systems, changing technology infrastructure, and their security is the impetus for identifying and modeling the management principles necessary to ensure access control.



Key Issues in the 1990's

1989		Issue Classification			
Rank	Issue Name	M/T	P/C	I/E	Group
1	Information Architecture	T	P	I	TI
2	Data Resource	M	C	E	BR
3	Strategic Planning	M	P	E	BR
4	IS Human Resources	M	C	I	IE
5	Organizational Learning	M	C	E	BR
6	Technology Infrastructure	T	C	I	TI
7	IS Organization Alignment	M	C	E	BR
8	Competitive Advantage	M	P	E	BR
9	Software Development	T	C	I	IE
10	Telecommunication Systems	T	C	E	TI
11	IS Role & Contribution	M	P	E	BR
12	Electronic Data Interchange	T	C	E	TI
12	Distributed Systems	T	C	E	TI
12	CASE Technology	T	C	I	TA
15	Applications Portfolio	T	C	I	IE
16	IS Effectiveness Measurement	M	C	I	IE
17	Executive/Decision Support	M	C	E	TA
18	End-User Computing	M	C	E	TA
19	Security & Control	T	C	I	IE
20	Disaster Recovery	T	C	I	IE
21	Organizational Structure	M	C	E	BR
22	Technology Islands	T	C	E	TI
23	Global Systems	M	P	E	TI
24	Image Technology	T	C	E	TA
25	IS Asset Accounting	M	C	E	BR

Note: Issues were classified as follows: "M/T" indicates management (M) or technology (T); "P/C" indicates planning (P) or control (C); "I/E" indicates internal (I) to IS organization or external (E); "Group" indicates business relationship (BR), technology infrastructure (TI), internal effectiveness (IE) or technology application (TA).

Figure 4.2: Information Systems Management Issues in the 1990's. Adapted from Fred Neiderman, James C. Brancheau and James C. Wetherbe, IS Management Issues in the 1990's. (Boulder, CO: University of Colorado Faculty Working Paper Series, 1990): 5.

NOTES - CHAPTER IV

1. Francis Misutka and Carl Stierson, "Infotech: Stand on Guard", Canadian Business (August 1989): 66.

2. Ibid.

3. John W. Verity, "Rethinking the Computer", Business Week (November 26, 1990): 117.

4. Ibid.

5. Ibid, 119.

6. Allan C. Utter, "The Four Essentials of Computer and Information Security", Internal Auditor (December 1989): 44.

7. Jonathan D. Harris and Gerald M. Ward, Managing Computer Risk: A Guide For The Policymaker, (New York: John Wiley and Sons, 1986): 32.

8. Ann Sussman, "Variety of Methods Are Best When Plugging Security Holes", PC Week (July 21.1989): 109.

9. Misutka and Stierson, 66.

10. Janet Mason, "It's Critical to Make PC Security as Flexible as the PCs Themselves", PC Week (March 15, 1988): 95.

11. Lee R. Alley and Stephan D. Willits, "ISDN: New Technology Poses Challenge to Auditors", Internal Auditor (February 1989): 14.

12. Carroll W. Frenzel, The Management of Information Technology, (Boulder, CO: N.P., 1990), 45.

13. Perry, William E, Management Strategies for Computer Security, (Boston: Butterworth Publishers, 1985), 137.

14. Jerome Lobel, Foiling the System Breakers (New York: McGraw-Hill Book Company, 1986), 94.

15. Ibid, 95.

16. Ibid, 92.

17. Kenneth P. Weiss, "Controlling the Threat to Computer Security", Management Review (June 1, 1990): 55.

18. Misutka and Stierson, 66.

19. Ibid.

20. James C. Brancheau, Fred Neiderman, and James C. Wetherbe, IS Management Issues in the 1990's, (Boulder, CO: University of Colorado Faculty Working Paper Series, 1990): 5.

21. Ibid, 10.

CHAPTER V

AN ACCESS SECURITY MANAGEMENT MODEL

Chapter Two described system access control as a subset of general business and IT controls which is critical to any overall IS security program. Chapter Three analyzed the threats to access security and found that eighty-percent of threats are internal, man-made errors, omissions or intentionally destructive acts. It also predicted a future increase in this human threat. Chapter Four described the fundamental architectural changes of distributed processing, how these changes effect access control, and the importance corporate IT managers place on distributed processing systems and security/control.

Access Security as a Management Problem

Technology does not control itself and so must be controlled by people within the firm. People, in turn, are controlled through proper management. The trend toward distributed systems allows more workers greater opportunities to access more information. As a result, integration and control of technology is becoming less a technology problem, and more a people problem.[1] Therefore, management must control technology by controlling its people.

Lobel proposed that most security access problems can be eliminated by controlling system access of workers within the firm. This adds credibility to the theory that access control is an internal management problem.

> Insiders with normal system access privileges are in a prime position (with enough technical expertise) to use computers for illegitimate purposes. Protecting against unauthorized access by an insider is therefore normally much more difficult than securing the system against an outsider. A system that is carefully safeguarded against unauthorized insider access should also be less vulnerable to an attack by an outsider.[2]

Access Security Devices

Although security devices are not the focus of this discussion, it is helpful to identify those available to management. Figure 5.1 is a partial list of the many technological devices available for controlling system access.

The technology to ensure access control is available. "The security provided is now good enough for most business purposes, provided that the systems are used in a secure manner. Unfortunately, this cannot always be guaranteed."[3] Therefore, management of this access technology is the key. Management must understand the distinction between technical security devices and the management practices which oversee their implementation. Ensuring proper use of security devices is the purpose behind system access control management.

Management Control Models

Now that the threats and management's role have been identified, and the available technology discussed, what specifically can management do to ensure proper control over access to their computer resources? It is simpler than many realize; for while the subject of access control is unique, most

TYPE OF DEVICE	DESCRIPTION
POSSESSION-RELATED DEVICES	**Allow access only if user has specific physical item**
Badges	
Tokens	
Card Keys	
Smart Cards	
Keyed Terminal Power Locks	
KNOWLEDGE-RELATED DEVICES	**Allow access only if user knows a secure access code**
Passwords	
Access Codes	
IDENTITY-RELATED DEVICES (BIOMETRICS)	**Allow access only if the user can be identified through physical means**
Signature Analysis	
Typing Analysis	
Hand Print Identification	
Voice Identification	
Retina Scanning Devices	
COMMUNICATION-RELATE DEVICES	**Prevent access of information via local or leased line communication links between network nodes**
Call-Back Devices	
Encrypting Devices	
Shielding	
Encasement	
DETECTION DEVICES	**Identify unauthorized access conditions and alert management**
AI-Based Intrusion Detection Systems	
Surveillance Equipment	
Light Beams	
Motion Detectors	

Figure 5.1: Access Security Technology

management principles for its control are common in planning and controlling other business functions.

Many concepts of security management controls already exist. Although different, these views of security control have common themes which serve as the basis for the management principles in my Access Control Management Model.

According to Boyce, general management control has four main purposes: to establish clear goals, to measure progress toward those goals, to indicate how to initiate corrective action, and to display potential areas for further improving the system.[4] To do this, four key planning items must be determined: what to measure, how to present the control information, what to consider critical issues, and who is accountable for controlling the information.[5]

> "From a management viewpoint, it is important to consider planning and control as complementary, and the one can hardly be dealt with without taking into account the requirements of the other."[6]

Ward and Harris focus Boyce's general view of control to the context of IT. They see management's role in data security as setting goals and standards, making supervisors responsible, providing adequate financial and personnel security resources, and measuring progress and performance against goals and standards.[7]

Findlay sees effective system control as a five-step process. First, because of the widespread propagation of IT, top management must assume overall responsibility for its control. Second, management must perform a risk analysis to specify threats. Third, management must identify security shortcomings by comparing the threats to existing controls. Next, management must communicate procedures to managers and workers within the firm (Findlay also recognizes insiders as the biggest threat to security). Finally, management must continuously monitor controls and reassess risks to ensure new gaps do not develop between threats and controls.[8]

The principles of accountability, prevention, detection, and enforcement form the control system proposed by Sweet. In Sweet's opinion accountability must be directed to users. "Responsibility or accountability for security should rest in the hands of those who own the data - the users. MIS can build the links, but users have to guard the chain."[9] Prevention includes the actual physical and logical controls devised to prevent unauthorized access. Detection involves procedures that go into effect when an unauthorized access is successful (for example, identifying the unauthorized user's location and dispatching security personnel to investigate). Finally, Sweet encourages variable enforcement of unauthorized accesses, based on the damage done.[10]

Burch and Sardinas see effective security resulting from accomplishment of five goals. There must be a deterrent to unauthorized access, then detection of unauthorized access similar to Sweet's principles. Third, there must be provisions developed to minimize the impact of an access breech. Investigation of circumstances surrounding the incident must be done. Finally, steps must be taken to recover lost resources if possible. [11]

Finally, Lobel's view of security involves six steps: understanding the need for access control, establishing a system security policy, selecting access control tools and technology, completing a secure system design, implementing and monitoring access control, and coping with change.[12]

An Integrated Access Control Management Model

The Access Control Management Model model devised for this research (see Figure 5.2) depicts a "ring" of system access control management. Actions based upon this model may effectively negate threat attempts to gain access to corporate data resources. The ring is comprised of several management functions which are supported by management tools. The model combines items from all the previously mentioned models. The management functions are repetitive in nature, from adjusting corporate thinking to system revision, with functions occurring generally in that sequence. The continuous nature of the model depicts management's need to adapt constantly to the dynamic IT environment. If the model's integrity is maintained through proper and continuous implementation of the functions and tools, the ring can ensure adequate control over access to IS both now and in the future.

The remainder of this chapter describes the elements of the Access Control Management Model:

Adjust Corporate Thinking

First, and sometimes most difficult, is the task of becoming organizationally aware of how systems have changed and how management thinking must also change. Traditional "mainframe mentality" is the enemy to this task. Executives in increasing numbers now possess a basic knowledge of IS and how they can be used to competitive advantage. However, many of these executives have not kept up with changes to the systems themselves, such as the architectural changes related to distributed IS.

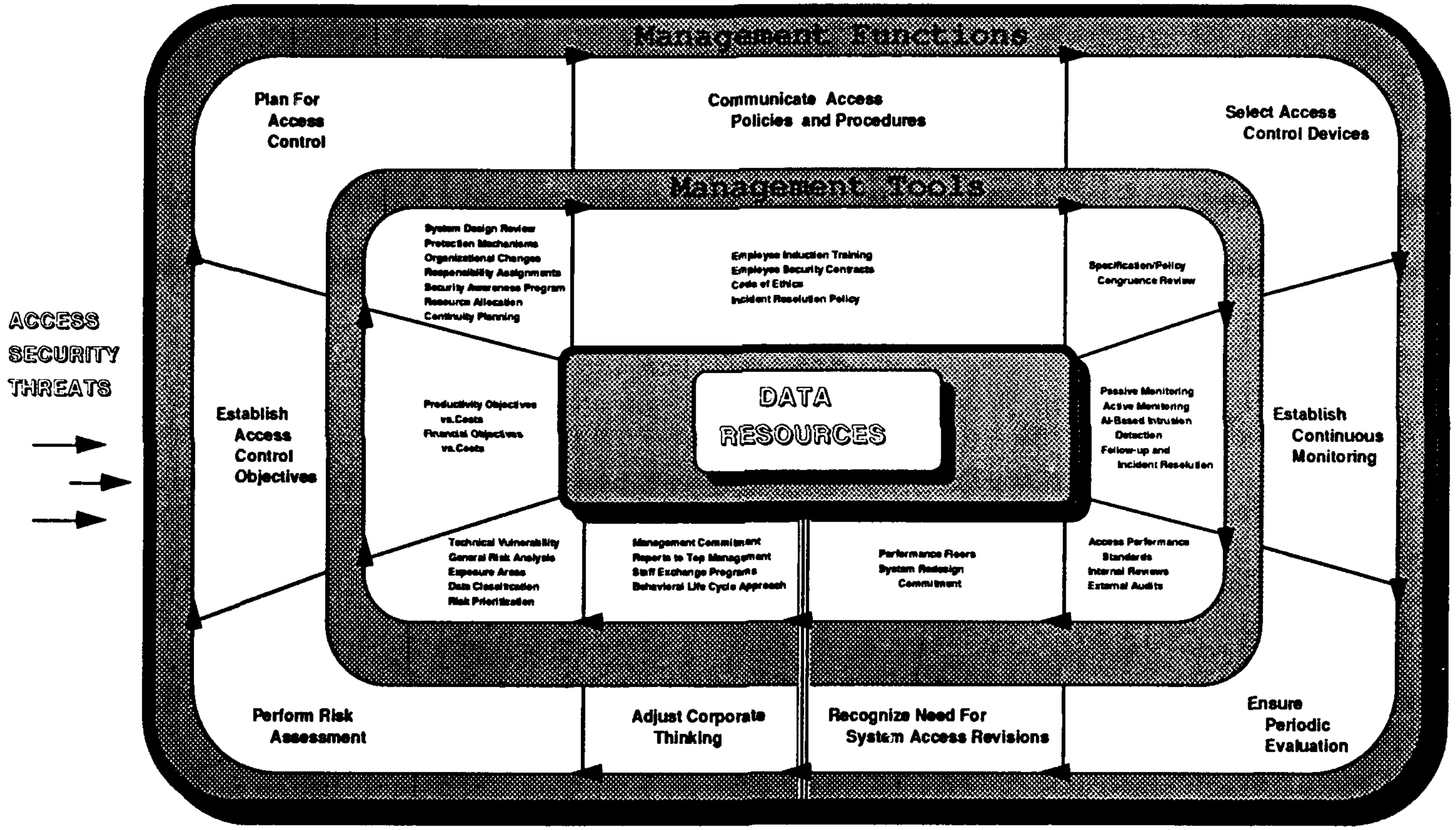

Management Functions
Plan For Access Control
Communicate Access Policies and Procedures
Select Access Control Devices
Establish Access Control Objectives
Establish Continuous Monitoring
Perform Risk Assessment
Adjust Corporate Thinking
Recognize Need For System Access Revisions
Ensure Periodic Evaluation
Management Tools
System Design Review
Protection Mechanisms
Organizational Changes
Responsibility Assignments
Security Awareness Program
Resource Allocation
Continuity Planning
Employee Induction Training
Employee Security Contracts
Code of Ethics
Incident Resolution Policy
Specification/Policy Congruence Review
Productivity Objectives vs.Costs
Financial Objectives vs.Costs
DATA RESOURCES
Passive Monitoring
Active Monitoring
AI-Based Intrusion Detection
Follow-up and Incident Resolution
Technical Vulnerability
General Risk Analysis
Exposure Areas
Data Classification
Risk Prioritization
Management Commitment
Reports to Top Management
Staff Exchange Programs
Behavioral Life Cycle Approach
Performance Floors
System Redesign Commitment
Access Performance Standards
Internal Reviews
External Audits
ACCESS
SECURITY
THREATS

Figure 5.2: Access Control Management Model

Updating management's, and subsequently workers', thinking is a long-term process that can only be done with support of the highest levels of management. "The top management is ultimately responsible for all security, including information and computer security. If management doesn't care, nobody else in an organization will."[13]

"The prevailing belief that most large organizations are suffering frequently from (....) assaults on information resources should put every information manager on red alert."[14] Spreading this alarm via top management is the initial challenge for the IT manager.

Three groups must change their thinking: top management, middle management, and users. Each group has its own background which distorts its view of system access security.

> Those charged with the responsibility for maintaining corporate resources - CEOs [Chief Executive Officers], CFOs [Chief Financial Officers], boards of directors - often have very little understanding of the degree of vulnerability they have with regard to computer security. Those charged with implementing computer technology, distributed systems and networks - primarily middle managers - are frequently overburdened, underbudgeted and often equally unaware of the real security issues. Those using the technology are concerned with user friendliness and have not been educated to the threat, potential methods of abuse, or the value of the information resources they are manipulating.[15]

Adopting a new way of viewing corporate access security will undoubtedly encounter some resistance. Humans are creatures of habit and changes are unsettling. Changes can be forced upon people, but true acceptance of the change may never take place.

A better process for encouraging change is much like the Behavioral Life Cycle used in preparing users for new IS. As Lewin points out through his model, successful social change takes form in three steps: unfreezing, moving, and refreezing. In unfreezing, people are prepared for an upcoming change. Moving represents the change itself. Refreezing involves feedback and further positive reinforcement of the change to ensure people do not return to the old way of doing things.[16]

Convincing top management that protecting their information resources is critical should not be a difficult task if the IT Manager presents figures on how much data is stored by corporate IT, and the results of security breakdowns in other presumably secure firms. In some cases, previous internal security breeches can help prompt a rethinking of security.

> Ironically, it may be the increasingly critical issues surrounding information security that force top management in many cases to view more seriously information as a resource, a commodity worth protecting, an often intangible asset which cannot be adequately insured against loss or destruction.[17]

Statistics emphasizing the insider threat also need to be presented to focus top-level managers on solving the human-factor problems, not just throwing more money into traditional, physically-oriented, technical security devices that work best in the more easily controlled mainframe environment.

Middle managers will usually follow the lead of top management. However, staff exchange programs can increase cooperation between IT and user departments, speeding the conversion from mainframe to distributed system thinking.[18] Adjustment of user thinking requires several other important steps later in the access control management process.

Perform Risk Assessment

To establish control that provides management's "steering function" it is first necessary to determine where the firm is with regard to access control. The purpose of risk assessment is to identify the general areas requiring improvements in security policies, administrative procedures, and technical safeguards.[19] A "tiger team" should simultaneously perform a technical vulnerability analysis to expose any technical shortcomings of hardware, software, and communication systems.

General risk assessment can be done by the firm's Data Security Department or by an outside consulting firm much the way accountants are hired to attend to financial procedures.[20] One such consulting firm, DMR Incorporated of Montreal, Canada, performs interviews with management and employees, and even distributes anonymous questionnaires to obtain a less biased view of current access security.[21]

Ideally, the assessment of risk should be done as a part of system design. The cost of risk assessment and resulting system modifications increases dramatically in the later phases of the system development life cycle. Existing systems must also be evaluated, however, security add-ons can be prohibitively expensive and may not interface as well as if the system was originally built around the necessary security measures.

The basic question of risk analysis is: "What needs protecting?" This can be done by determining the potential value of data to users and competitors, the cost of nonavailability to the firm, any legal protection requirements, and possible embarrassment resulting from divulged data.[22]

Ward and Harris apply this same question in five key exposure areas: operational dependence (the ability to continue operations), financial implications, financial reporting implications (harm to financial statements), information sensitivity, and system structure (the architecture of the system). Answers vary depending on the size of the firm and the type, size, and functionality of the system used (mainframe, stand-alone, or distributed network systems).[23]

After determining what type of harm unauthorized access will do, data should be classified by its overall value in accordance with internal management conventions. One such system is the Industrial Security Manual For Safeguarding Classified Information (ISM) used by commercial defense contractors.[24] Data is classified as confidential, secret, or top secret depending on whether damage, serious damage, or grave damage to national security would result from data compromise. Firms without Department of Defense ties can modify this to reflect damage to the firm's security, reputation, or competitive advantage.

Next a risk factor, or probability of exposure, must be assigned. Although this is highly subjective for items such as reputation or embarrassment, they, and other more objective items such as downtime, can and must be quantified. Risk factors are computed as the expected loss (in dollars) multiplied by the probability of exposure (as a percentage).[25] Proper control measures minimize computed risk by lowering exposure or expected losses. The result of risk analysis should be a clear view of what information is in need of protection and the ramifications if that information, or the ability to use it, are compromised.[26]

Once risks are computed, they can be prioritized by management. Some risks may be too high to accept, and the business function modified. Other risks may deserve more attention than others to significantly lower overall risk to the firm. Finally, some risks are acceptable and not worth additional outlays to lower them.

Once the business assets to be protected are identified, and the exposures and potential for loss of those assets are evaluated, controls can be designed and implemented to achieve security control objectives.[27]

Establish Access Control Objectives

Security control objectives provide the answer to the following question: "What are we trying to accomplish?" "The issue to be addressed by management is not whether an organization should implement data security, but how far on the security continuum [the] organization needs to travel."[28]

Again, firms with Department of Defense contracts must follow mandated security procedures with equipment approved by the National Security Agency.[29] Firms which do not contract with the government must determine their own appropriate level of security.

Two costs must be balanced with the potential risk factors identified during risk assessment: productivity and financial.

Authorized user access is the productivity concern:

> Too much security makes access harder. Management perceives hard access as a lack of service, and so do some customers. On the other hand, management is also responsible for security, which sets up an interesting (and possibly troublesome) dichotomy.[30]

Access barriers must prevent unauthorized use while allowing authorized persons to efficiently access needed programs and data. "Users don't want technology, they want solutions to business problems."[31] IT managers are not in the data processing or IS business, they are in the business of making their users successful. Access security must not hamper the performance of users significantly or they will circumvent the controls, leaving the firm as vulnerable as if there were no controls at all.

The cost of access security must also be reasonable. It makes no sense to spend more on security measures than the firm would lose if security were compromised. Even incremental security costs should be justified by an equal or greater offset in potential loss or risk.

Because of these two costs, total access security is realistically unattainable. A totally secure system would cost so much to implement it would more than offset any cost savings realized by the system. Likewise, a totally secure system would hinder performance to such a point that the system would make users unproductive. The manager's challenge is to find the highest point at which access security is increased without similar or greater increases in cost or decreases in productivity.

Plan For Access Control

The access security plan answers: "How do we accomplish these security objectives?" This plan should detail how to effectively solve the problems uncovered in risk assessment.

System Design Review.

Access security must become an integral part of system design. Security must be at the forefront of all system development and subsequent modifications if risks are to be reduced at the lowest cost. All departments should review every system's access security characteristics and how these fit into existing corporate programs prior to implementation.[32]

Protection Mechanisms. Another important part of access control planning is determining the protection mechanisms for access control. Protection mechanisms are not security devices, but tenants or theories behind how security devices can be effectively implemented.

For example, the protection mechanism for stand-alone systems should combine both physical and logical security aspects, although physical measures are generally most effective. Physical access can be controlled by locating stand-alone PCs in restricted access areas such as a common PC room or a locked private office. Restricted physical access has the added benefit of reinforcing separation of duties (only those workers authorized to access data on certain stand-alone units will have a key to the room).[33] Most stand-alone PCs have only limited logical access control. Additional password protection packages are available, but are expensive to provide for all individual systems.

If PCs are linked to a host mainframe or other server, but have no communication capabilities (local area networks), the logical aspects of control become more of a concern. Although physical access control measures can be taken, network nodes may not be located in the same secure area, creating a greater probability of data access. Logical access to the nodes can be controlled via the main server, making expensive individual terminal logic access controls unnecessary. However, overly restrictive access controls will effect the performance of not just one user, but all users on the network. The final protection mechanism implemented may be multi-faceted if varieties of system types exist within the overall corporate IS.

Choosing appropriate protection mechanisms alsc relates to the two cost factors examined while establishing control objectives.

Performance has historically been the emphasis in the IT industry. Improvements in size, speed and capability of microprocessors have been exponential. There are only a handful of microprocessor designs left; those that survived have done so on the basis of their performance. "It is clear that a solution to security problems must be found within that context."[34]

Performance being a paramount concern, an easy way to provide logical security would be to limit access control to initial log-in procedures and ease subsequent security:

> It is better to think in terms of secure enclaves on the perimeter of which strict security is enforced. Within the enclave there is a lower degree of security or perhaps none at all. This model of security is applicable to distributed systems, in particular to groups of work stations with file servers. These can be surrounded by a security barrier within which there is a relaxed attitude to security.[35]

The security devices listed in Figure 5.1 have the capability to thwart most any unauthorized access attempt. The key is how well they are applied.

> The biggest impediment to providing appropriate security in today's environment isn't technological - it is perceived cost and convenience. A cost-effective increase in the level of security - one that doesn't burden either the user or the program manager - is needed. We need to maintain the convenience and flexibility of a simple password and, at the same time, exponentially increase its security.[36]

This increased security can be provided at a reasonable cost by two-factor authentication systems. There are three widely-accepted methods of authenticating potential users: something known to the user, something the user keeps, and some unique user attribute. Passwords, tokens, and signatures are respective examples of these methods. Two-factor authentication, recommended by the National Bureau of Standards, uses any two of the three methods in tandem before allowing a user access to the system.[37]

Initial access is better controlled with two-factor authentication than with simple passwords. In order to not further complicate security, the biometric or known authentication variables can be automatically entered into an access control matrix which holds the specific file and function authorizations for the particular user. Only those files, applications, or functions (update, read, delete, or create) the user has specific permission to perform will be made available to the user.[38]

No other access security is necessary within this "secure enclave". Additional security measures would only tend to slow productivity and frustrate users. "Indeed, it is hard to see any other way in which a group of work stations could be made secure, since there is not [a] central operating system."[39]

When networked PCs/workstations have communication capabilities (wide area networks) extra measures are needed to prevent remote log-ins. During normal business hours remote log-ins should not be allowed. Someone within the "secure enclave" should authenticate the user on an external channel before allowing access. After hours, call-back devices, and challenge-response devices should be used to authenticate potential system users. Encrypting transmitted data is another method to help prevent unauthorized tapping of corporate or dial-up network communication links.

Organizational Changes. Because of the proliferation of computers throughout the firm, any security effort must be both coordinated and standardized. Many firms have begun this effort in regard to PC procurement, maintenance, and user interface by organizing Workstation Stores and Information Centers. Similarly, security can be centralized through creation of a Director of Security Office which reports to top management. The Director of Security would have staff responsibility for coordinating and standardizing corporate-wide security efforts. This includes access security which can be specifically controlled by the Data Security Officer within the IT Department.[40]

Use of PCs, whether networked or stand-alone, can be monitored and improved by creating an IT Advisory Committee made up of user department representatives. The purpose of this group is to improve existing automation via suggestions and prioritized work requests.[41]

Yet another IT department, the Network Responsibility Center, should rise from the increased use of telecommunications.[42] This center is essential for any firm whose strategy includes telecommunications for competitive advantage. The Network Responsibility Center's mission is to manage the links between data terminal equipment throughout the firm. Steve Dreyer, president of the Systems Methods Associates consulting firm, states:

> There must be a network group in a large organization where there are complex communication functions. The telecommunication problems and planning in these organizations probably can not and should not be handled by groups responsible for applications and systems development.[43]

Many other high-level IT managers agree with this viewpoint and urge the separation of network and IT management. However, the close relationship between telecommunication networks and IT necessitates the inclusion of the Network Responsibility Center in the Director of Security's and IT Manager's area of control.

Responsibility Assignments. Once proper organizational structure is determined, top-level management must assign responsibilities to these organizations to ensure all aspects of access security are covered.[44] One possible division of responsibilities is shown in Figure 5.3. Specific functional responsibilities will vary according to the organization's size and security strategy.

Security Awareness Program. After involving top-level management and structuring middle-level management, the next step is to involve corporate users through a security awareness program. This involves periodic internal training programs which detail expected security conduct (ethics), how to use security devices, and the overall positive effect of security on protecting the company (and therefore the employees) from financial ruin. The program may also include written notices concerning specific security problems as needed.

American Computer Security, a security consulting firm, goes one step further by encouraging client managers to steal all disks/information left unsecured at the end of the day. When workers return the next day they discover they can't continue working without the stolen items. This "false crisis" has proven very effective at promoting physical security and backing up of data.[45]

Resource Allocation. Even a well-designed plan will fail if financial, personnel, and time resources are not assigned to implement it. Top management holds the key to resources and should allocate them based on the earlier objective-cost analysis.

This may not always be happening, however. A survey of eighty-six Fortune 500 companies in 1988 by Datamation magazine found more than half

TOP MANAGEMENT

- Provides appropriate organizational structure
- Establishes security policies and approves standards
- Allocates resources
- Requires periodic reports on security and integrity

USER DEPARTMENT MANAGERS

- Ensure training of users in security and integrity procedures
- Enforce top management's policies and standards

PERSONNEL DEPARTMENT

- Screens employees before training

INTERNAL AUDIT DEPARTMENT

- Assesses adequacy of security and integrity safeguards

MIS ADVISORY COMMITTEE

- Makes policy recommendations for all MIS activities
- Monitors adequacy of controls in all MIS activities

DIRECTOR OF SECURITY

- Establishes procedures for implementing security policies and standards
- Assigns responsibility for assessment of risks and safeguards
- Prepares contingency plans
- Reports on security to top management

DATA SECURITY OFFICER

- Implements and monitors data security and integrity practices
- Institutes procedures to authenticate access to data files and programs
- Issues and changes passwords for MIS users

Figure 5.3: Responsibilities For Data Security and Integrity

of the companies allotted less than one-half of one percent of their IT budget to security. Another third of the companies budgeted between one-half and one percent for security.[46] This is an indicator that top-level management have not universally focused their thinking and efforts toward security and that their IT managers must adjust corporate thinking.

Continuity Planning. Finally, provisions must exist in the overall access security plan to ensure proper monitoring, evaluation, and revision programs are in place. These will be detailed in subsequent sections of this chapter.

Communicate Access Policies and Procedures

Policies and procedures are the backbone of any access control system. They are the detailed steps that ensure accomplishment of security objectives.

"There is no such thing as a bullet-proof system and humans are the weakest link in the security chain. Security experts repeatedly point out that the key to good security is a set of procedures."[47]

Access security policies and procedures are important because they represent the link between management edicts and employee actions. However, they are effective only if the employees know about them.

> A survey by Price Waterhouse found that fewer than 50% of businesses communicated these policies to users outside the data processing area. Management's expectation of data safeguarding must be clearly communicated to the employees.[48]

This means having formal, written documentation for employee reference, backed up by periodic training (such as a security awareness program). Communication should begin immediately upon hiring an employee. "Perhaps, as a very first rule, any good corporate security policy should be conveyed to employees as part of their induction training."[49]

Employee intent to comply with standards should be documented by having each employee sign a contract that they understand the firm's security desires. The employee contract should detail the exact meaning of what is considered company information. "A contract clause that restricts employees from copying, securing, transmitting, keeping, storing, gaining from, selling, or using company information" will clearly define what employees can and cannot do.[50] Information must also be defined to include data, programs, techniques, and processes. Finally the contract should spell out what action the firm will take against employees who violate standards.

Catholic University of America in Washington, D.C. takes a slightly different approach to this idea. In its "code of ethics", Catholic University attempts to educate all students, faculty and employees on rules regarding computer use as well as punishment for misuse. Although users are not required to actually sign any document, Ardoth Hassler, the university's Assistant Director of Academic Computing, states: "In the event that we do have a problem, it gives us something to stand on, a foundation on which to base your work or punishment."[51]

A critical follow-up to the communication of policies to employees is the administration of an incident resolution policy for non-compliance. This involves administrative action, legal action, or both.

Minor infractions of access security policies warrant administrative action. This involves tying employee access security performance to periodic performance appraisals. If, for example, an employee leaves a password unsecured (and securing passwords is in the employee's written responsibilities) the immediate supervisor should note it on the employee record. Multiple access violations may lead to comments on a performance appraisal which could have detrimental effects during the employee's next salary review.[52]

Major violations, such as deliberate unauthorized access require swift legal actions. Dismissal, or at least immediate restricted access from all computer resources may be in order. This is where the tight coordination between all departments spelled out in the access security plan comes into play. The System Security Officer must ensure all departments are informed, from the employee's department to the personnel department, and even to the security guards at the entrance to the building. Information dissemination procedures must ensure everyone is aware of the restriction/termination and the possibility of backlash from the employee.

The firm must be ready to follow-up tenaciously with legal action to deter future violations. Many corporations fail to do this and simply fire offending employees.

> Businessmen either don't want to suffer the public embarrassment which may result in a loss of confidence in the company, or they're afraid that the company information the thief was trying to steal will become public information.[53]

However, most everyone now realizes data compromise is occurring at an increasing rate. A blank prosecution record should lead investors to conclude there are weak controls, not that there have been no violations. If businesses fail to follow up, "borderline ethical" employees may decide the potential gain of unauthorized activities outweighs the minimal risk presented by corporate policies and actions. In the broad sense, punishment acts as a general deterrent to future violations.

Both administrative and legal measures rely on measurable criteria for violations.[54] For instance, a generated report displaying an unauthorized access or a confiscated "tickler note" with an employee's password can serve as proof of infractions. These details must be considered prior to enacting a tough incident resolution policy.

Other critical policies such as new employee background screening, the time interval for periodic access control training for employees, and issuance and control of passwords or other authentication devices must also be detailed so all aspects of access control are formalized and enforced.

Select Access Control Devices

Access control plans and policies provide a basis for selecting security devices that limit access to corporate data resources. Specifications for the devices must reflect corporate access control policies. Because specifications lead to the procurement of access security devices, the specifications should address problems identified during risk assessment and detail how these problems will be solved.

Management review of specifications ensures congruence with policies. This is especially important if the specifications are developed by a technical "tiger team" or by outside consultants. Perhaps a better way to create appropriate specifications is with a team headed by the System Security Officer that includes managers, technicians, and users.[55]

Establish Continuous Monitoring

Access monitoring is essential to prevent, detect, and report any unauthorized activity related to the IS. Monitoring is accomplished by an access surveillance system, usually part of the system's access control software.[56] This monitoring can be active or passive. Passive monitoring ensures unauthorized access attempts are denied and that subsequent reports showing the attempted access are printed. Although necessary, this is "after-the-fact" security. Active monitoring takes steps to alert proper authorities while stalling the unauthorized user by means of special, extended dialogues.[57] Effective access monitoring systems should employ both active and passive features for human and computer-initiated access attempts.

How does this relate to management? Monitoring systems are designed and implemented much the same way access control devices are chosen. Management from all levels must have input to desired features of the monitoring system and work closely with outside security consultants or internal security teams to ensure proper controls are included. Only management can ensure the access monitoring system includes a combination of active and passive monitoring controls. Management must decide how passive reports are formatted so they contain all critical exception information, and do not become just another data-intensive report nobody can read or understand. Management must initiate active monitoring measures such as checking known hacker electronic bulletin boards, to ensure the firm is not targeted for compromise.[58]

Management should also keep abreast of potential monitoring improvements. For example, both the Navy and Air Force are currently testing intrusion detection using expert systems to identify unusual access attempts compared to established employee access patterns. Citicorp financial services currently uses similar monitoring for its invoice system.[59] Although currently too expensive for many firms, management should study and consider it for future implementation when justified by access control objective-cost analysis.

Management must also be involved in follow-up when access violation feedback is generated by the system. Access violations involving critical corporate assets require top level management involvement.[60]

Finally, management's willingness to prosecute violators per the corporate incident resolution policy is critical. The best policy and monitoring controls can be undermined by management timidity or fear of adverse publicity. No system can be an effective deterrent without aggressive follow-up by management.

Ensure Periodic Evaluation

Performance is assured by management evaluation to determine how well current access controls are performing. This implies a comparison of actual events to measurable standards of performance. These performance standards are developed from access control objectives and the detailed specifications used for access control device selection.

Management must create a program that effectively evaluates access controls against performance criteria. The program must be periodic, accurate, and provide an unbiased view of access controls. This requires use of both internal and external system reviews.

The internal review team is management's eyes and ears for access control. The members of this team must be skilled in both IT and internal controls, and must be aware of corporate organization, objectives, and procedures. Finally, they must create an open, working relationship with corporate management and IS users.

Management's role is to first create this team and hire qualified staff, then support its mission and assist in establishing the internal review system as a positive part of access control and IT operations. This last role is perhaps most important as access control can be realized only if all players are working, in concert, toward the same access security goals.

Internal review of access controls can be performed by the firm's Data Security Department. The main functions of internal review are to assess system functionality and then certify access controls are in place. Internal reviewers are best qualified to assess technical functionality because they are more familiar with specific access controls built into the IS, as well as the firm's programming and analysis techniques, and documentation. They are also as much there to "sell" the access control program to users as they are to evaluate it.[61]

Outside auditors should evaluate the non-technical aspects of access control and provide an unbiased, overall view of their effectiveness. Management, IS personnel, and the internal review team should assist by clarifying access control objectives, explaining operating procedures, and providing access control documentation and reports.

Recognize Need For System Access Revision

Management cannot overlook the final management function: revision. If management follows the previously discussed principles, it can control system access effectively. However, control can only be considered effective in the current time frame. Management must realize that change is constant and the changing environment will eventually undermine the effectiveness of current controls. Revision is very similar to adjusting corporate thinking in that it involves attitudes toward access controls and change.

Belden Menkus discussed this management function in regard to what he calls the "law of increasing entropy" which recognizes that IS are constantly moving toward disorder.[62]

To succeed in dealing with this natural tendency, Menkus suggests management first resign itself to the fact that implementation is not the final step in system development. Management should accept the thought that access controls will deteriorate over time. Management must determine measurable system performance floors and periodically evaluate system performance against these objectives to determine when entropy has rendered access controls ineffective. At this point, management must also be aware that they should devote additional resources to maintain or completely redesign the access controls.[63]

The revision function brings management full circle and prepares the organization to meet future access control challenges. This research has concentrated on distributed systems involving networked PCs. This environment will surely be replaced with still more advanced environments in the future. Management must be prepared to continually adapt its access control thinking and perform the discussed functions if it is to survive changes beyond the current horizon.

An Initial Judgement of the Model

After constructing my model, I discovered additional corroborating research. Straub and Hoffer's 1988 study of contemporary information security methods outlined six steps for forming a computer security administration function.[64] These steps are: development of a security/disaster recovery plan, development and dissemination of electronic data processing guidelines, conducting employee security orientation programs, classification of information/programs/records, selection of security monitoring packages, and finally constant monitoring and reassessment of security packages. The same study also emphasized proper organization, and clear and frequent communications as effective deterrents to unauthorized access.

Straub and Hoffer's conclusions were based on 1,211 survey responses from members of the Data Processing Management Association. The similarity of their six-step process to the principles behind the access control management model, and the extent of their study, increases confidence that the model's content is valid.

The Overall Principles

This chapter discussed the management functions and tools depicted in the model, relating them to the distributed processing environment. However, this model can apply to any significant change in IT, not just the change from mainframe to distributed systems. Since access control is central to a total security program, this model should also be modifiable to this expanded scope.

Although the management tools used to implement this process are somewhat unique, the basic management principles of setting objectives, planning, communicating, monitoring, evaluating, and revising apply to many other functional areas as well as to access controls.

The Access Control Management Model points out IT management's overall responsibility to provide a uniform focus on access controls from an organization-wide perspective, and to themselves focus on the human aspect of access security.

> Above all, cooperation throughout the organization will be required. As many people as possible need to be involved in the evolution of such controls: this will help achieve an acceptance of their aims and will assist in providing a corporate balance and objectivity.[65]

If this focus is achieved, all managers and users must be constantly challenged to support the program's objectives. "The best [security] systems are only as good as their implementation. They rely on people to make them work."[66]

Management must be cautious not to believe that even a well-planned and executed access security program is impermeable. "There is no such thing as security; there are only varying degrees of insecurity."[67] Management's role in access control is to identify, control, and manage this insecurity at a level acceptable to the firm.

> The groundswell of abuse is not the end of the computer's usefulness, nor is it the beginning of the end, but perhaps it is the harbinger of management's appropriate sensitivity, awareness and responsibility for computer security policies.[68]

The alarming trends in computer insecurity may bring thoughts of the decline of the information age. However, I believe security is simply a new factor among the multitude of critical success factors for today's corporate managers.

NOTES - CHAPTER V

1. Richard K. Aeh, "Technology Integration, Agents of Change and a New IS Culture", Journal of Systems Management (October 1989): 20.

2. Jerome Lobel, Foiling the System Breakers (New York: McGraw-Hill Book Company, 1986), 3.

3. Maurice V. Wilkes, "Computer Security in the Business World", Communications of the ACM (April 1990): 399.

4. R.O. Boyce, Integrated Managerial Controls: A Visual Approach Through Integrated Management Information Systems (New York: American Elsevier Publishing company, 1968), 37.

5. Ibid.

6. Ibid.

7. Gerald M. Ward and Jonathan D. Harris, "Data Security: Ten Tough Questions", Research and Development (March 1987): 25.

8. Grant Findlay, "Data Security: Reducing the Risks", The Accountant's Magazine (June 1987): 58.

9. Frank Sweet, "How to Build a Security Chain", Datamation (February 1, 1987): 70.

10. Ibid.

11. John G. Burch and Joseph L. Sardinas, Computer Control and Audit: a total systems approach (Santa Barbara: Wiley and Sons, 1978), 217.

12. Lobel, 7.

13. Allan C. Utter, "The Four Essentials of Computer and Information Security", Internal Auditor (December 1989): 44.

14. Kevin Wilson, "Coping With Computer Crime", Records Management Quarterly (July 1989): 56.

15. Kenneth P. Weiss, "Controlling the Threat to Computer Security", Management Review (June 1, 1990): 55.

16. Per O. Flaatten, Donald J. McCubbrey, P. Declan O'Riordan, Keith Burgess, Foundations of Business Systems (Chicago: The Dryden Press, 1989), 37.

17. Wilson, 58.

18. Ward and Harris, 25.

19. Lobel, 69.

20. Chris Terry, "Hardware and Software Keep Your PC Safe", EDN (September 1, 1989): 63.

21. Janet Mason, "It's Critical to Make PC Security as Flexible as the PCs Themselves", PC Week (March 15, 1988): 93.

22. Lobel, 14.

23. Gerald M. Ward and Jonathan D. Harris, Managing Computer Risk: A Guide for the Policymaker (New York: John Wiley and Sons, 1986), 33.

24. Lobel, 64.

25. Donn B. Parker, Computer Security Management (Reston: Reston Publishing company Incorporated, 1981), 40.

26. Ann Sussman, "Variety of Methods Are Best When Plugging Security Holes", PC Week (July 21, 1989): 109.

27. Robert K. Harman and Robert D. Neary, "Planning Your Microcomputer Security Strategy", Financial Executive (April 1987): 10.

28. Ward and Harris, 26.

29. Terry, 61.

30. Utter, 44.

31. Aeh, 20.

32. Ward and Harris, 25.

33. J.L. Bookholdt, "Controlling Your Desktop Computers", CMA - The Management Accounting Magazine (October 1989): 51.

34. Maurice V. Wilkes, "Computer Security in the Business World", Communications of the ACM (April 1990): 400.

35. Ibid.

36. Weiss, 56.

37. Sussman, 109.

38. Lobel, 86.

39. Wilkes, 400.

40. Bookholdt, 54.

41. Ibid.

42. Steve Dreyer, "Telecommunication and MIS: Managing the Merger", *Datamation* (October 15, 1985): 122.

43. Ibid.

44. Bookholdt, 53.

45. Mason, 93-95.

46. Ali F. Farhoomand and Michael Murphy, "Managing Computer Security", *Datamation*, (January 1, 1989): 67.

47. Terry, 83.

48. Ward and Harris, 25.

49. Peter Nota, "Data Manipulation in a Secure Environment", *Accountancy* (June 1989): 142.

50. Francis Misutka and Carl Stierson, "Infotech: Stand on Guard", *Canadian Business* (August 1989): 68.

51. Michael Alexander, "Keep 'Em Honest", *Computerworld* (March 27, 1989): 42.

52. Michael Alexander, "Holding Your End Users Accountable", *Computerworld* (May 1, 1989): 42.

53. Misutka and Stierson, 68.

54. Alexander, "Keep 'Em Honest", *Computerworld* (March 27, 1989): 42.

55. Lobel, 208.

56. Ibid, 253.

57. Ward and Harris, 26.

58. Ibid.

59. Susan Kerr, "Using AI to Improve Security", *Datamation* (February 1, 1990): 57.

60. Lobel, 259.

61. Mary M. Lee, "The Challenge of EDP Auditing", *Management Accounting* (March 1988): 52.

62. Belden Menkus, "It's Only Natural That Things Continue to Get Worse", Journal of Systems Management (October 1989): 5.

63. Ibid.

64. Detmar W. Straub and Jeffrey A. Hoffer, Computer Abuse and Computer Security Administration: A Study of Contemporary Information Security Methods, (Bloomington, IN: Indiana University Institute For Research in the Management of Information Systems Working Paper #W801, 1988), 47.

65. Nota, 143.

66. Mason, 95.

67. Utter, 44.

68. Sweet, 59.

CHAPTER VI

RESEARCH METHODOLOGY

This chapter focuses on the research to validate the access control management model developed in Chapter Five. The chapter is broken into sections explaining selection of research participants and conduct of research.

Research Participants

Possible participants fell into one of three categories: those presently using distributed processing, those switching from centralized to distributed systems, and those contemplating the switch. Because the management functions in the model included later stages of access control management (evaluation and revision), these aspects could not be addressed by participants presently switching to distributed systems. Those who had only plans to convert to distributed systems were also ruled out because the model would be better scrutinized by comparison to actual experience, rather than conjecture or feelings.

As the model's components were not technical or overly specialized, participant industry and location were not considered significant to the results. Management is fairly consistent no matter where, or in what environment it is performed. Considering time and budget constraints, it was deemed prudent to consider participants in the Colorado Front Range regardless of industry.

Managers were the most obvious participants for the survey. However, IT practitioners in non-management positions also have important roles in determining the corporate access security process. Therefore, the only requirement for participating in the survey (other than being in a firm which had implemented distributed systems) was to be in a position that related to the development, operation, or evaluation of access security.

Conduct of the Research

I contacted prospective participants through several IT-oriented organizations: the Denver Chapters of the Association of Contingency Planners, Electronic Data Processing Auditors Association, Information Security Society of America, and Data Processing Managers Association.

A main research concern involved how best to acquire information to validate the management model, considering the potentially sensitive nature of IS security topics such as access control. Many firms rely upon IT to gain competitive advantage. Probing into the security aspects of those systems would likely meet with resistance.

Conferring with marketing faculty helped determine that questionnaires offered the highest degree of anonymity while still providing the information needed to validate the model. Questionnaires would also help minimize the effects of interview bias by ensuring every participant was asked the same questions.

Despite the anonymity of the questionnaire, I suspected without personal contact to gain the trust of participants, the response rate would likely be very low. Therefore, I made an effort to visit a monthly meeting of each organization to introduce myself and personally explain the purpose of my research.

As expected, I found all four organizations generally reluctant to provide information about security. Everyone I talked to, without exception, was concerned with the type of questions they would have to answer. Even generic questions were acceptable only if they had no specific ties to their work. Because of this the final questionnaire was designed to address strictly management model elements, and not to determine security specifics of the participants' organizations.

Two organizations offered to have me personally present my model and research topic to its members at monthly meetings. The presentation was restricted to an outline of administrative aspects of the study and a brief explanation of the model so as not to bias the participants. This initial conversation emphasized the scope of the research as being management related, not specifically security related. Participants were assured total confidentiality if desired. Questionnaires were distributed at the meetings to those in the target category who indicated they would participate.

The other groups' meeting formats were not appropriate for my presentation, and so contacts were made with group officers who agreed to release member information for questionnaire mailings.

The questionnaire allowed participants the opportunity to clarify their answers via a follow-up interview. If they supplied a phone number, these participants were contacted by phone.

Questionnaire Structure

Because of the sensitive nature of the topic, questions applied directly to the management model. The structure of the questionnaire allowed participants to rank and sequence the model's components, and identify any omissions or extraneous components. Finally, participants were given a chance to rate the model's current and future usefulness.

The research executive summary, questionnaire, and survey packet appear in Appendix A.

CHAPTER VII

SUMMARY DISCUSSION OF SURVEY FINDINGS

Despite my personal efforts, response rates were low. A total of eighty-six questionnaires were distributed with twenty-four returned for a 27.9 percent response rate. Although disappointing, the low response is not surprising due to the sensitive nature of the research topic.

Participant Profile

Information pertaining to survey participants includes job titles and experience level. Figure 7.1 shows the job titles of respondents. The average time as a manager was 4.75 years, with a range of zero to fifteen years. The seven respondents with no management experience were in positions directly related to security development (Data Security Administrator) or security evaluation (Senior EDP Auditor). The average time associated with information technology was 12.67 years, with a range of two to twenty-five years. This shows that those responding generally had considerable experience in the industry. Seven respondents were members of the Information Security Society of America, three were from the Electronic Data Processing Auditors Association, eight were from the Data Processing Managers Association, and six were from the Association of Contingency Planners.

JOB TITLE

President

Vice President

Vice President, Information Systems

Controller

Information Security Manager

Data Security Administrator

Security Administrator

Manager, Computer Security

Director, Computer Services

Principle Systems Analyst

Operations Management Specialist

DataBase/Local Area Network Administrator

Local Area Network Manager

Program Specialist

Senior Customer Coordinator

Senior Electronic Data Processing Auditor

Audit Senior Manager

Contingency Planner

Operations Compliance Manager

System Engineer

Data Control Administrator

Figure 7.1: Job Titles of Respondents

Because of measures taken to protect the anonymity of participants, no information about company type or size is available. However, this information is insignificant in validating the model.

Of the twenty-four respondents, nine included a phone number on the survey indicating they would like to further discuss their answers. Another six returned their addresses so they could receive a copy of the research results.

Summarized survey results are in Appendix B.

The Model

Utility

Overall, participants responded very favorably to the model. 87.5 percent felt access control could be effectively managed using the model's principles. 95.8 percent agreed with the concept that access control management is a repetitive process as shown in the model. With regard to distributed processing, 95.8 percent said that model would either definitely or probably be useful. 100 percent thought the model would be of use for future IT environment changes.

Structure

Again, most responses indicated the model was complete. 79.2 percent felt the model's functions were all inclusive; 90.4 percent felt similarly about the supporting management tools. Only two suggestions for additional functions or tools were similar, dealing with threat analysis. Suggestions for functions included defining asset ownership, risk assessment testing, threat analysis, disaster recovery/integrity, and research/analysis of new technology.

Requests for additional tools indicated separation of duties, cross training, and state of threat analysis should be added.

Participants unanimously agreed that all model components were important enough to be part of the model. There were no specific requests to delete any element.

Element Importance

Although most responses agreed the overall structure of the model was appropriate, answers varied about the importance of individual functions and tools.

The average response for all management functions was well above seven on a scale of ten. Adjusting corporate thinking was most critical (9.0) while selecting access control devices was least critical (7.8). More importance was placed on the earlier stages of the model than the latter (see Appendix B-1).

Seven management tools failed to rank higher than seven out of ten in degree of support to their respective management functions. Staff exchange programs, the behavioral life cycle approach, organizational changes, employee security contracts, passive monitoring, artificial intelligence-based intrusion detection, and external audits were not considered as effective as other tools by survey participants.

The highest degree of support ratings were given to management commitment, exposure areas, risk prioritization, follow-up and incident resolution, technical vulnerability analysis, resource allocation, internal review, and system design review (see Appendix B-2).

Sequence

Another point of contention was the order in which management should perform the access control functions. 58.3 percent felt the model's sequence was correct. The remaining participants had varying views of how the functions should be rearranged.

After averaging all responses, however, the respondents' sequencing corresponded surprisingly well with the original access control management model (see Appendix B-3). This was due to several response generalities found even in the responses calling for changes.

86.3 percent of responses agreed that the first function and the last three functions should remain in the sequence shown in the model. 95.5 percent agreed that establishing objectives should be done prior to control planning.

Adjusting corporate thinking was sequenced either first or second in all but four cases. In two of these cases it was placed last in sequence. However, both these respondents also believed access management was repetitive in nature. In this context, adjusting thinking can either be first or last in the process depending on the perspective of the manager. This was confirmed with both respondents who ranked adjusting corporate thinking last in telephone interviews. Thus, in my analysis, rankings of one or nine for adjusting corporate thinking were considered similar.

In all but one case, communicating access policies and procedures was sequenced after the first four functions. However, only 72.7 percent of respondents sequenced communicating access policies and procedures before selecting access control devices. Similarly, only 77.3 percent sequenced risk assessment ahead of establishing access control objectives.

Corporate Practices

Participants' organizations did tend to use the management functions and tools in the model (see Appendix B-4). Of participants choosing to respond (three did not, presumably because of the nature of the topic), implementation of the model's management functions ranged from 57.1 percent (ensuring periodic evaluation) to 90.5 percent (establishing access control objectives). Overall function management implementation was 72.5 percent. This indicates basic security principles as shown in the model are more often than not being addressed by participants' firms.

The implementation of management tools covered a much broader range (see Appendix B-5). Only 11.1 percent indicated they used staff exchange programs, while 72.2 percent indicated system design review was part of their access security programs. Overall implementation for the model's management tools was 45.6 percent. The difference between this and the higher implementation of management functions may be accounted for by the fact that more than one tool is associated with each function (firms that implement a function may not use all the supporting tools associated with that function).

However, these figures say nothing about the effectiveness of these business practices. One respondent commented that policy, practice, and procedures dictate that all functions and tools should be done, but adherence to them is questionable.

Caveats

Survey responses may be distorted by respondent bias. Those who took the time to respond may have done so because they were positively impressed with the model. Those who were not may have had a greater tendency not to respond.

The way the data was collected may also have introduced bias to the results. All participants were members of professional IT groups. The fact that they belong to such groups may indicate a greater than average interest in security which may have exaggerated implementation and support rankings, and implementation rates.

Finally because of the small sample size, final results reacted significantly to individual responses outside the normal distribution. A greater sample size would have decreased the sensitivity of individual data and increased the confidence of the results considerably. Therefore, the reader should not attempt to extrapolate this small sample to represent fact for larger environments. What may be true from the survey responses may not be true of businesses, or even Front Range businesses as a whole. Responses indicate only how the surveyed practitioners viewed the management of system access control.

CHAPTER VIII

FINAL ACCESS CONTROL MANAGEMENT MODEL

Despite the possible biases, the positive reaction to the model indicates only minor changes are necessary (see Figure 8.1).

Management functions received positive support overall. Most suggestions for additions were corollaries to management tools already in the model. Asset ownership, for example, is a part of responsibility assignments. Management should assign responsibility for each asset (application program, data store, hardware, etc.) in the organization. Risk assessment testing is done throughout risk assessment to determine where vulnerability exists. Research and analysis of new technology fits well into recognizing the need for system access revisions. Finally, threat analysis determines who or what may exploit any vulnerability discovered through risk assessment. Although these suggestions are similar to tools in the original model, they do convey a different perspective and therefore are included in the revised model. Suggestions for additional management tools included separation of duties, cross training, and state of threat analysis. Separation of duties falls under the category of responsibility assignment and is in fact one of the goals behind assigning responsibilities. State of threat analysis was already added to the revised model. Cross training is covered by staff exchange programs, however, the respondent indicated his company did not use that tool. The overall low implementation and low importance rankings given to staff

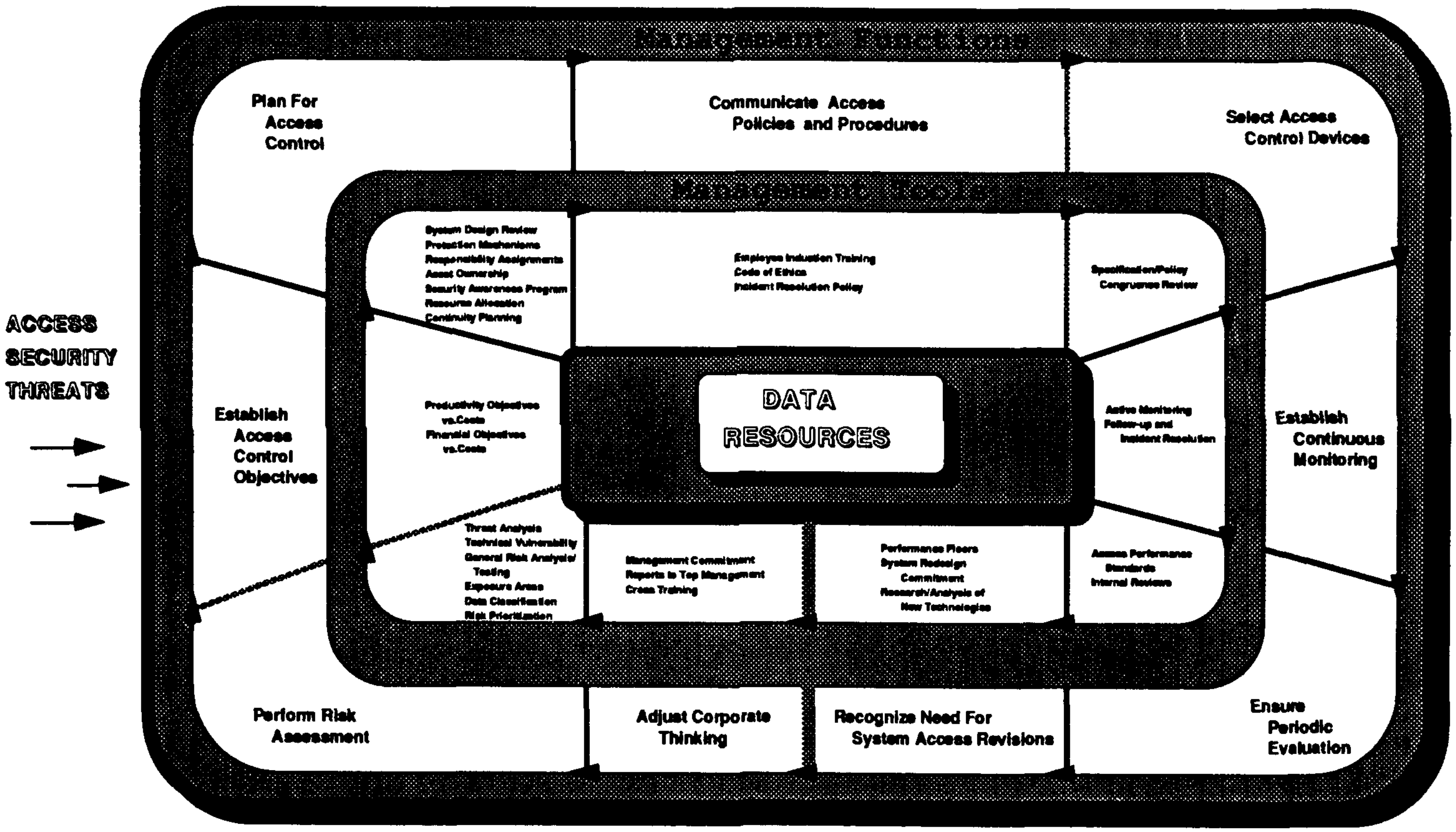

ACCESS
SECURITY
THREATS
Management Functions
Plan For Access Control
Communicate Access Policies and Procedures
Select Access Control Devices
Establish Access Control Objectives
Establish Continuous Monitoring
Perform Risk Assessment
Adjust Corporate Thinking
Recognize Need For System Access Revisions
Ensure Periodic Evaluation
Management Tools
System Design Review
Protection Mechanisms
Responsibility Assignments
Asset Ownership
Security Awareness Program
Resource Allocation
Continuity Planning
Employee Induction Training
Code of Ethics
Incident Resolution Policy
Specification/Policy Congruence Review
Productivity Objectives vs.Costs
Financial Objectives vs.Costs
Active Monitoring
Follow-up and Incident Resolution
Threat Analysis
Technical Vulnerability
General Risk Analysis/ Testing
Exposure Areas
Data Classification
Risk Prioritization
Management Commitment
Reports to Top Management
Cross Training
Performance Floors
System Redesign Commitment
Research/Analysis of New Technologies
Assess Performance Standards
Internal Reviews
DATA
RESOURCES

Figure 8.1: Revised Access Control Management Model

exchange programs, coupled with this apparent confusion over terminology indicated a need to change the tool's name to cross training. Because of the possible misunderstanding, I decided not to delete this tool.

A similar correlation between relative importance and implementation was seen in several other management tool rankings. Behavioral life cycle approach, organizational changes, employee security contracts, and AI-based intrusion detection ranked low in both categories. Because these tools were neither considered critical nor used, they were deleted from the final model.

Two tools, passive monitoring (61.9 percent implementation) and external audits (52.3 percent implementation), were implemented to a greater extent than one would expect from their low support rankings. This led to the conclusion that although used more often than not, these tools were considered ineffective and should not be included as essential components of the management model (interestingly, a Senior EDP Auditor gave external audits the lowest support ranking!).

Finally, participants' firms were not using several tools as much as they should be as evidenced by support rankings. Technical vulnerability analysis (8.3 support ranking and only 38.8 percent implementation), incident resolution policy (7.7 and 33.3 percent), specification/policy congruence reviews (7.5 and 19.0 percent), access performance standards (7.6 and 33.3 percent), and performance floors (7.3 and 23.8 percent), were implemented in under forty percent of firms surveyed despite support rankings above seven out of ten. These tools may be the most important ones to retain in the model because they were not used in the majority of surveyed firms.

Sequencing of the original model was determined to be appropriate. Less than half of the responses indicated changes were needed, these changes were mostly minor, and no two changes matched. When all responses were averaged, the overall sequence remained the same (see Appendix B-3).

However, three management function pairs were close enough to consider revising the model. The first of these was between adjusting corporate thinking and recognizing the need for system access revision (where the repetitive management cycle begins and ends). There were differing opinions whether adjusting corporate thinking was first or last in sequence. In light of this, the distinct vertical start/stop line in the original model was "blurred" in the updated model.

Two other functional borders were also blurred. The first was between risk assessment and control objectives. 22.7 percent of total responses switched the sequence of these functions. One respondent explained his sequencing by stating: "You can't perform risk assessment without understanding [control objectives]". Another respondent in a follow-up telephone interview, called the sequencing a "chicken and egg" situation, pointing out that risk is not valid unless it is part of business control objectives. Second, 27.2 percent reversed the sequence of communicating policies and procedures with selecting access control devices. The communication function was the most variant, placed anywhere from second to ninth in sequence by the respondents. However, its sequence was most often switched with selecting access control devices.

With these incorporated changes, the final access control management model better reflects the real world views of IT practitioners. It is interesting, perhaps somewhat comforting, to see the similarity to the original scholarly model. This may suggest that the two worlds of academia and business are more harmonious than many believe.

CHAPTER IX

RESEARCH CONCLUSIONS

Conclusions

This research presented a graphical depiction of the management process related to IS access control. The scholarly research model was reviewed and commented on by a variety of IT practitioners from Colorado Front Range organizations. Incorporated revisions brought the model closer to what practitioners felt was a functional access control management process.

This research led to several positive conclusions. First, access control can be distilled into a number of management functions and supporting tools, as evidenced by the resounding positive response from survey respondents. Second, access control management, like other aspects of management is likely an iterative, continuous cycle with no clear beginning or end. This process is considered useful in guiding change from mainframe to distributed systems, and also in guiding future access-related IT changes. Fourth, surveyed businesses implement all of the model's management functions and tools to an extent, but not always proportionate to the element's perceived impact on control. There is evidence that passive monitoring techniques and external audits, both reactive tools, may not be effective tools for access control. Other evidence indicates more proactive tools such as technical vulnerability analysis, incident resolution policies, specification/policy congruence reviews, access performance standards, and performance floors may be effective if included in more corporate access control programs.

Future Research Directions

The low response rate may indicate the reluctance of the IT community to discuss security practices, even on a general level. Perhaps personal interviews or group sessions would have elicited more response. Nevertheless, the limited data gathered encourages further validation of the model in a broader environment, perhaps using a different survey technique.

One question that was never directly answered was whether access control is a management or technology problem. The conclusion reached from scholarly research (that access control is a management problem) was never solidified with survey evidence.

Another potential research project could be to tie the security history of an organization to its access control management practices. It may be possible in this way to validate whether the model ensures success or not.

A final direction holds the most promise. One respondent commented that access control is but a subset of security and one must address much more, such as integrity and disaster recovery. No one would dispute this, however, this research purposely concentrated on the access subset because it is the building block for total IS security. In a follow-up telephone conversation the respondent agreed that other security subsets would be inappropriate in this model, but might also be modeled along with a higher-level model of total IS security. Such a group of models may provide a simplified way of tackling the broad and complicated area of IT security and control.

BIBLIOGRAPHY

Aeh, Richard K. "Technology Integration, Agents of Change and a New IS Culture." Journal of Systems Management (October 1989).

Alexander, Michael. "Keep 'Em Honest." Computerworld (March 27, 1989).

Alexander, Michael. "Holding Your End Users Accountable." Computerworld (May 1, 1989).

Alley, Lee R. and Stephan D. Willits. "ISDN: New Technology Poses Challenge to Auditors." Internal Auditor (February 1989).

Anthony, Robert N., John Dearden and Norton M. Bedford. Management Control Systems. Homewood, IL: Richard D. Irwin Incorporated, 1989.

Bidgoli, Hussein and Reza Azarmsa. "Computer Security: New Managerial Concern for the 1980's and Beyond." Journal of Systems Management, (October 1989).

Bookholdt, J.L. "Controlling Your Desktop Computers." CMA - The Management Accounting Magazine (October 1989).

Boyce, R.O. Integrated Managerial Controls: A Visual Approach Through Integrated Management Information Systems. New York: American Elsevier Publishing Company, 1968.

Brancheau, James C., Fred Neiderman and James C. Wetherbe. IS Management Issues in the 1990's. (Boulder, CO: University of Colorado Faculty Working Paper Series, 1990).

Burch, John G. and Joseph L. Sardinas. Computer Control and Audit: A Total Systems Approach. Santa Barbara: Wiley and Sons, 1978.

Burgess, Keith, Per O. Flaatten, Donald J. McCubbrey, and P. Declan O'Riordan. Foundations of Business Systems. Chicago: The Dryden Press, 1989.

Cashin, James A. Management Controls. Hempstead, NY: Hofstra University Yearbook of Business, Series 4, Volume 2, 1967.

Dreyer, Steve, "Telecommunication and MIS: Managing the Merger." Datamation (October 15, 1985).

Farhoomand, Ali F. and Michael Murphy. "Managing Computer Security." Datamation (January 1, 1989).

Findlay, Grant. "Data Security: Reducing the Risks." The Accountant's Magazine (June 1987).

Frenzel, Carroll W. The Management of Information Technology. Boulder, CO: N.P., 1990.

Gilbert, Jerome. "Computer Crime: Detection and Prevention." Journal of Property Management (March-April 1989).

Hafner, Katherine M. "Is Your Computer Secure?" Business Week (August 1, 1988).

Harman, Robert K. and Robert D. Neary. "Planning Your Microcomputer Security Strategy." Financial Executive (April 1987).

Harris, Jonathan D. and Gerald M. Ward. "Data Security: Ten Tough Questions." Research and Development (March 1987).

Harris, Jonathan D. and Gerald M. Ward. Managing Computer Risk: A Guide for the Policymaker. New York: John Wiley and Sons, 1986.

Kerr, Susan. "Using AI to Improve Security." Datamation (February 1, 1990).

Lee, Mary M. "The Challenge of EDP Auditing." Management Accounting (March 1988).

Lobel, Jerome. Foiling the System Breakers. New York: McGraw-Hill Book Company, 1986.

Maciariello, Joseph A. Management Control Systems. Englewood Cliffs, NJ: Prentice-Hall Incorporated, 1981.

Makley, William K. "Computer Security's Worst Enemy: Management Apathy." The Office (March 1987).

Mason, Janet. "It's Critical to Make PC Security as Flexible as the PCs Themselves." PC Week (March 15, 1988).

Menkus, Belden. "It's Only Natural That Things Continue to Get Worse." Journal of Systems Management (October 1989).

Misutka, Francis and Carl Stieren. "INFOTECH: Stand on Guard." Canadian Business (August 1989).

Nota, Peter. "Data Manipulation in a Secure Environment." Accountancy (June 1989).

Parker, Donn B. Computer Security Management. Reston: Reston Publishing Company Incorporated, 1981.

Perry, William E. Management Strategies for Computer Security. Boston: Butterworth Publishers, 1985.

Schwartz, Melvin. "Computer Security: Planning to Protect Corporate Assets." The Journal of Business Strategy (January-February 1990).

Straub, Detmar W. and Jeffrey A. Hoffer. Computer Abuse and Computer Security: A Study of Contemporary Information Security Methods. (Bloomington, IN: Indiana University Institute for Research in the Management of Information Systems Working Paper #W801), 1988.

Sussman, Ann "Variety of Methods Are Best When Plugging Security Holes." PC Week (July 21, 1989).

Sweet, Frank "How to Build a Security Chain." Datamation (February 1, 1987).

Terry, Chris. "Hardware and Software Keep Your PC Safe." EDN (September 1, 1989).

Utter, Allan C. "The Four Essentials of Computer and Information Security". Internal Auditor (December 1989).

Verity, John W. "Rethinking the Computer." Business Week (November 26, 1990).

Webster's Third New International Dictionary, Unabridged. G&C Merriam Company, 1976.

Weiss, Kenneth P. "Controlling the Threat to Computer Security." Management Review (June 1, 1990).

Wilkes, Maurice V. "Computer Security in the Business World." Communications of the ACM (April 1990).

Wilson, Kevin. "Coping With Computer Crime." Records Management Quarterly (July 1989).

APPENDIX A

RESEARCH SURVEY PACKET

RESEARCH PROJECT

MANAGEMENT OF INFORMATION TECHNOLOGY ACCESS CONTROLS

EXECUTIVE SUMMARY

Objective:

This research attempts to determine the management principles important to ensuring an appropriate level of information system access control throughout the firm. Information technology managers' experience and opinions will be used to validate a previously prepared model depicting these management principles. This research does not concentrate on the specific mechanisms of a firm's security, but is simply an attempt to determine what functions management believes are important to developing and maintaining access security within organizations.

Research Participants:

Information technology managers from various firms using distributed information systems. Participation in this research is completely voluntary.

Data Collection:

Information will be collected via questionnaire with possible phone interview follow-up. The questionnaire is shown on subsequent pages.

Participant Time Requirement:

The enclosed questionnaire has been designed to reduce the time required and should take no more than fifteen minutes to complete. If a follow-up conversation is needed, it will be done over the phone as quickly as possible.

Confidentiality:

Participants do not have to answer questions with which they feel uncomfortable and can withdraw from the survey at any time. All names and company identities will be withheld from the report. Research materials will be stored under lock and key in the Office of the Director of Business Research. All research materials will be destroyed upon completion of the research.

Participant Benefits:

Interviewees will receive a copy of research results, if name and address are provided on the questionnaire. The research summary should provide information not readily available through ordinary operational means.

Graduate School of Business Administration
University of Colorado, Boulder 80309-0419
Research Director: Dr. Carroll Frenzel (303) 492-8227
Graduate Researcher: Michael Pollack (303) 652-2816

DEFINITIONS

The following are explanations of terms and phrases that may be unfamiliar or used in unique context.

Access Control Devices - For example, badges, tokens, passwords, voice identification, encryption devices, motion detectors, surveillance equipment, etc.

Adjust Corporate Thinking - Becoming organizationally aware of how information systems have changed and how the management of those systems must also change.

Behavioral Life Cycle - Preparing for, and ensuring the success of change introduced to organizations through a three-step process of "unfreezing", changing and "refreezing" attitudes and behavior.

Distributed Information System - The new architecture of information system consisting of microcomputers networked to specialized minicomputer servers.

Exposure Areas - Five factors that help management determine "what needs protecting" by identifying the type of exposure: operational dependence (ability to continue operations), financial implications, financial reporting implications(harm to financial statements), information sensitivity, and system structure (the architecture of the information system).

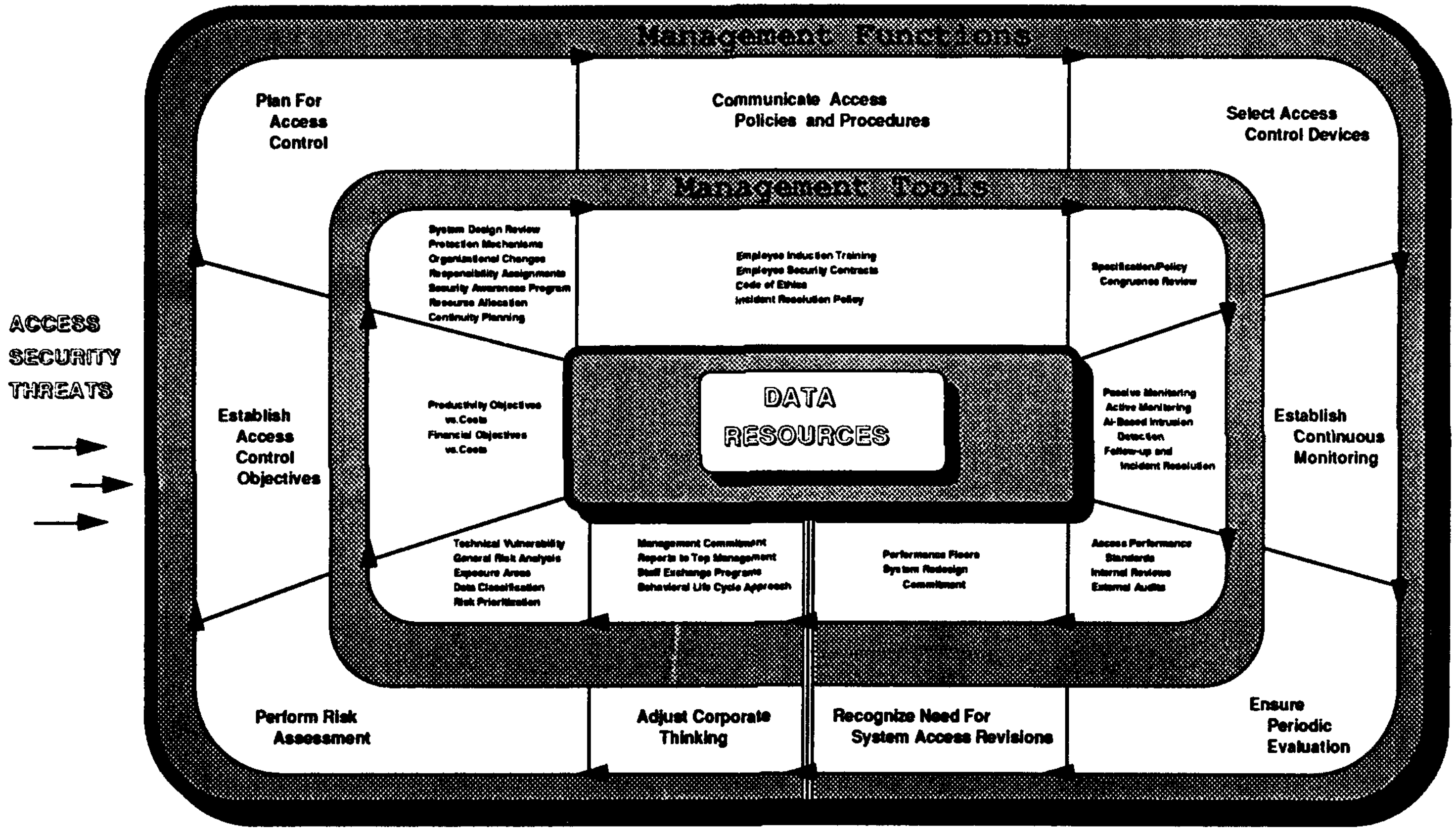
Incident Resolution Policy - A corporate policy that mandates review and follow-up of all access violations. This policy may also encourage legal action against unauthorized users.

Information System - This includes all manual and automated aspects of information processing such as policies, procedures, hardware, software and telecommunications.

Protection Mechanisms - The tenants or theories behind implementing access controls. For example, stand-alone microcomputers can be successfully secured through mostly physical security measures such as restricted use areas. Access to networked microcomputers with telecommunications capabilities must also be secured through logical security measures such as passwords, biometrics or call-back devices.

Performance Floors - Minimum acceptable standards of system performance that indicate to management when system enhancement is needed.

System Access Control - The application of policies and procedures for directing, regulating and coordinating the ability to enter or communicate with a network for collection and distribution of information.


ACCESS
SECURITY
THREATS
Management Functions
Plan For Access Control
Communicate Access Policies and Procedures
Select Access Control Devices
Establish Access Control Objectives
Establish Continuous Monitoring
Perform Risk Assessment
Adjust Corporate Thinking
Recognize Need For System Access Revisions
Ensure Periodic Evaluation
Management Tools
System Design Review
Protection Mechanisms
Organizational Changes
Responsibility Assignments
Security Awareness Program
Resource Allocation
Continuity Planning
Employee Induction Training
Employee Security Contracts
Code of Ethics
Incident Resolution Policy
Specification/Policy Congruence Review
Productivity Objectives vs.Costs
Financial Objectives vs.Costs
DATA RESOURCES
Passive Monitoring
Active Monitoring
AI-Based Intrusion Detection
Follow-up and Incident Resolution
Technical Vulnerability
General Risk Analysis
Exposure Areas
Data Classification
Risk Prioritization
Management Commitment
Reports to Top Management
Staff Exchange Programs
Behavioral Life Cycle Approach
Performance Floors
System Redesign Commitment
Access Performance Standards
Internal Reviews
External Audits

This model depicts a "ring" of system access control management that negates threat attempts to gain access to corporate data resources. The ring is comprised of several management functions, which are supported by management tools. The management functions are repetitive in nature, starting from adjusting corporate thinking to system revision. The continuous nature of the model depicts management's need to adapt constantly to the dynamic information technology environment.

QUESTIONNAIRE

The following questions relate to the management model on the previous page.

1. Do you feel access control of distributed information systems can be effectively managed using general management principles like the ones depicted in the model? _____ yes _____ no

If no, what is wrong with applying these principles? ____________________

____

2. Does the concept of repetitive management functions and tools make sense as depicted in the model? _____ yes _____ no

If no, how should the model be changed? ____________________

____

3. Please rate the importance of the following management functions to maintaining access control for information systems (*circle your response*):

	Degree of importance									
Management function	Not needed at all						Critical for success			
__ Adjust corporate thinking	1	2	3	4	5	6	7	8	9	10
__ Perform risk assessment	1	2	3	4	5	6	7	8	9	10
__ Establish access control objectives	1	2	3	4	5	6	7	8	9	10
__ Plan for access control	1	2	3	4	5	6	7	8	9	10
__ Communicate access policies and procedures	1	2	3	4	5	6	7	8	9	10
__ Select access control devices	1	2	3	4	5	6	7	8	9	10
__ Establish continuous monitoring	1	2	3	4	5	6	7	8	9	10
__ Ensure periodic evaluation	1	2	3	4	5	6	7	8	9	10
__ Recognize the need for access revisions	1	2	3	4	5	6	7	8	9	10

4. Please circle those management functions above that your firm performs.

5. Are these functions in the proper sequence? _____ yes _____ no

If no, please number the management functions from one to nine (one represents first in sequence) in the spaces provided to the left of each function.

6. Should any other functions be added? _____ yes _____ no

If yes, specify the functions ______________________________

7. Should any functions be deleted? _____ yes _____ no

If yes, specify the functions ______________________________

8. Please indicate the extent to which the following management tools support the nine management functions from the model (*circle your response*):

Management function Management tools	Degree of support Very Little									Very Great
Adjust Corporate Thinking										
Management Commitment	1	2	3	4	5	6	7	8	9	10
Reports to Top Management	1	2	3	4	5	6	7	8	9	10
Staff Exchange Programs	1	2	3	4	5	6	7	8	9	10
Behavioral Life Cycle Approach	1	2	3	4	5	6	7	8	9	10
Perform Risk Assessment										
Technical Vulnerability Analysis	1	2	3	4	5	6	7	8	9	10
General Risk Analysis	1	2	3	4	5	6	7	8	9	10
Exposure Areas	1	2	3	4	5	6	7	8	9	10
Data Classification	1	2	3	4	5	6	7	8	9	10
Risk Prioritization	1	2	3	4	5	6	7	8	9	10
Establish Access Control Objectives										
Productivity Objectives vs. Costs	1	2	3	4	5	6	7	8	9	10
Financial Objectives vs. Costs	1	2	3	4	5	6	7	8	9	10
Plan For Access Control										
System Design Review	1	2	3	4	5	6	7	8	9	10
Protection Mechanisms	1	2	3	4	5	6	7	8	9	10
Organizational Changes	1	2	3	4	5	6	7	8	9	10
Responsibility Assignments	1	2	3	4	5	6	7	8	9	10
Security Awareness Program	1	2	3	4	5	6	7	8	9	10
Resource Allocation	1	2	3	4	5	6	7	8	9	10
Continuity Planning	1	2	3	4	5	6	7	8	9	10

Management function Management tools	Degree of support									
	Very Little						Very Great			
Communicate Access Policies and Procedures										
Employee Induction Training	1	2	3	4	5	6	7	8	9	10
Employee Security Contracts	1	2	3	4	5	6	7	8	9	10
Code of Ethics	1	2	3	4	5	6	7	8	9	10
Incident Resolution Policy	1	2	3	4	5	6	7	8	9	10
Select Access Control Devices										
Specification/Policy Congruence Review	1	2	3	4	5	6	7	8	9	10
Establish Continuous Monitoring										
Passive Monitoring	1	2	3	4	5	6	7	8	9	10
Active Monitoring	1	2	3	4	5	6	7	8	9	10
AI-Based Intrusion Detection	1	2	3	4	5	6	7	8	9	10
Follow-Up and Incident Resolution	1	2	3	4	5	6	7	8	9	10
Ensure Periodic Evaluation										
Access Performance Standards	1	2	3	4	5	6	7	8	9	10
Internal Reviews	1	2	3	4	5	6	7	8	9	10
External Audits	1	2	3	4	5	6	7	8	9	10
Recognize the Need For System Access Revisions										
Performance Floors	1	2	3	4	5	6	7	8	9	10
System Redesign Commitment	1	2	3	4	5	6	7	8	9	10

9. Please circle the management tools your firm uses.

10. Should any other tool(s) be added? _____ yes _____ no

If yes, what function(s) do(es) the tool(s) support?

Tool ______________________ **Function** ______________________

Tool ______________________ **Function** ______________________

11. **How useful would you consider this model for distributed systems?**

____ **Definitely useful**
____ **Probably useful**
____ **Probably not useful**
____ **Definitely not useful**

12. **How Useful Could The Model Be For Future Changes?**

____ **Definitely useful**
____ **Probably useful**
____ **Probably not useful**
____ **Definitely not useful**

13. **What is your position/title?** ________________________________

14. **How long have you been a manager?** ______ **years**

15. **How long have you been associated with information technology?** ______ **years**

16. **If you would like a copy of the research summary, please print your name and address in the space below.**

____

____

____

____

17. **If you would be willing to participate in a short telephone interview to clarify your answers, please print your phone number in the space below.**

____

I very much appreciate your time and effort in helping with this research. If you are mailing this, please return [illegible] four questionnaire sheets only.

APPENDIX B

QUESTIONNAIRE SURVEY RESULTS

Management Function	Degree of importance									
	Not needed								Critical	
	1	2	3	4	5	6	7	8	9	10
Adjust corporate thinking (9.0)									X	
Perform risk assessment (8.4)								X		
Establish access control objectives (8.7)									X	
Plan for access control (8.2)								X		
Communicate access policies and procedures (8.1)								X		
Select access control devices (7.8)								X		
Establish continuous monitoring (8.0)								X		
Ensure periodic evaluation (8.1)								X		
Recognize the need for access revisions (8.0)								X		

Appendix B-1: Management Function Degree of Importance

Management Function Management Tool	Degree of Support									
	Very Little							Very Great		
	1	2	3	4	5	6	7	8	9	10
Adjust Corporate Thinking										
Management Commitment (8.8)									X	
Reports to Top Management (7.1)							X			
Staff Exchange Programs (5.3)					X					
Behavioral Life Cycle Approach (5.9)						X				
Perform Risk Assessment										
Technical Vulnerability Analysis (8.3)								X		
General Risk Analysis (7.8)								X		
Exposure Areas (8.5)								X		
Data Classification (7.1)							X			
Risk Prioritization (8.5)								X		
Establish Access Control Objectives										
Productivity Objectives vs. Costs (7.8)								X		
Financial Objectives vs. Costs (7.9)								X		

Appendix B-2: Management Tools Degree of Support

Management Function Management Tool	Degree of Support									
	Very Little							Very Great		
	1	2	3	4	5	6	7	8	9	10
Plai. For Access Control										
System Design Review (8.3)								X		
Protection Mechanisms (8.0)								X		
Organizational Changes (5.8)						X				
Responsibility Assignments (7.4)							X			
Security Awareness Program (7.6)								X		
Resource Allocation (8.1)								X		
Continuity Planning (7.5)							X			
Communicate Access Policies and Procedures										
Employee Induction Training (7.5)							X			
Employee Security Contracts (6.5)						X				
Code of Ethics (7.2)							X			
Incident Resolution Policy (7.7)								X		

Appendix B-2: Management Tools Degree of Support (continued)

Management Function Management Tool	**Degree of Support**									
	Very Little							**Very Great**		
	1	2	3	4	5	6	7	8	9	10
Select Access Control Devices										
Specification/Policy Congruence Review (7.5)								X		
Establish Continuous Monitoring										
Passive Monitoring (7.0)							X			
Active Monitoring (7.9)								X		
AI-Based Intrusion Detection (6.7)							X			
Follow-Up and Incident Resolution (8.4)								X		
Ensure Periodic Evaluation										
Access Performance Standards (7.6)								X		
Internal Reviews (8.1)								X		
External Audits (6.3)						X				
Recognize the Need For System Access Revisions										
Performance Floors (7.3)							X			
System Redesign Commitment (7.4)							X			

Appendix B-2: Management Tools Degree of Support (continued)

MANAGEMENT FUNCTION	AVERAGE SEQUENCE
Adjust corporate thinking	1.2
Perform risk assessment	2.1
Establish access control objectives	2.8
Plan for access control	3.8
Communicate access policies and procedures	5.1
Select access control devices	5.7
Establish continuous monitoring	6.9
Ensure periodic evaluation	7.9
Recognize the need for access revisions	8.7

Appendix B-3: Respondent Sequencing of Management Functions

MANAGEMENT FUNCTION	PERCENT IMPLEMENTATION
Establish Access Control Objectives	90.5
Establish Continuous Monitoring	76.2
Communicate Access Policies and Procedures	76.2
Plan For Access Control	76.2
Adjust Corporate Thinking	71.4
Recognize the Need For System Access Revisions	71.4
Perform Risk Assessment	66.7
Select Access Control Devices	66.7
Ensure Periodic Evaluation	57.1

Appendix B-4: Use of Management Functions by Respondents

MANAGEMENT TOOL	PERCENT IMPLEMENTATION
System Design Review	72.2
Exposure Areas	66.7
Management Commitment	66.7
Protection Mechanisms	66.7
Internal Reviews	61.9
Passive Monitoring	61.9
General Risk Analysis	61.1
Security Awareness Program	55.5
Financial Objectives vs. Costs	55.5
Responsibility Assignments	55.5
Productivity Objectives vs. Costs	55.5
Employee Induction Training	52.4
Active Monitoring	52.4
External Audits	52.4
Risk Prioritization	50.0
Continuity Planning	50.0
Data Classification	50.0
Resource Allocation	50.0
Reports to Top Management	44.4

Appendix B-5: Use of Management Tools by Respondents

MANAGEMENT TOOL	PERCENT IMPLEMENTATION
Code of Ethics	42.8
Follow-Up and Incident Resolution	42.8
Technical Vulnerability Analysis	38.8
System Redesign Commitment	38.1
Incident Resolution Policy	33.3
Employee Security Contracts	33.3
Access Performance Standards	33.3
AI-Based Intrusion Detection	28.6
Organizational Changes	27.7
Performance Floors	23.8
Behavioral Life Cycle Approach	22.2
Specification/Policy Congruence Review	19.0
Staff Exchange Programs	11.1

Appendix B-5: Use of Management Tools by Respondents (continued)