A Socio-Technical Perspective on Information Security Knowledge and Attitudes

Approved by
Dissertation Committee:

Rajendra K. Srivastava, Co-Supervisor

E. Glynn Harmon, Co-Supervisor

Allucquere Rosanne Stone

Larry R. Leibrock

M Erin Porter

M. Erin Porter

A Socio-Technical Perspective on Information Security Knowledge and Attitudes

by

Cheri Lanette Long, B.A., M.A.

Dissertation

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

Doctor of Philosophy

The University of Texas at Austin

May, 1999

UMI
300 North Zeeb Road
Ann Arbor, MI 48103

Socio-Technical Perspective on Information Security Knowledge and Attitudes

Publication No.____________

Cheri Lanette Long, Ph.D
The University of Texas at Austin, 1999

Supervisors: E. Glynn Harmon and Rajendra K Srivastava

Too often managers regard computer security as a technology problem rather than a management one. In an annual Information Security Survey, Ernst & Young found agreement on basic information security issues. However, despite the heightened awareness of security issues, the survey found that many companies had serious gaps in their security. Although eighty percent of respondents said winning the commitment of top management is the key to improving information security, management appears to have only a superficial understanding of security.

Although research has been conducted that measures attitudes toward information security of executives, little research has been carries out that measures actual knowledge of information security concepts among future

Information Management executives. This research looks at the degree of security knowledge of information security concepts and its relationship to security attitudes of Information Management candidates enrolled in an Information Management graduate program of a nationally ranked graduate school of business.

The study shows a low level of knowledge of the technical requirements for establishing information security despite the respondents rating information security issues as highly important. The author concludes that an increased emphasis on information security education in business education is needed. In addition there is a need to raise management's awareness of the issues involved in implementing information security in an organization. Until business education in information security successfully equips future managers to provide meaningful oversight, the deficiencies must be made up through the education of existing management.

This research concludes by recommending the incorporation of information security concepts throughout the range of Information Management undergraduate and graduate curricula as well as addressing the deficiencies of current management through Executive Education Programs.

Table of Contents

CHAPTER I

GENERAL PROBLEM STATEMENT

> It may roundly be asserted that human ingenuity cannot concoct a cipher which human ingenuity cannot resolve.
>
> – Edgar Allan Poe

Advances in computer and communication technologies have enabled the evolution of new forms of information exchange.[i] Much has changed in the last twelve to twenty four months in the way that people and organizations work. Many organizations are making information available because it helps them to secure a critical advantage over their competitors, is a way of delivering better service to their customers and/or is a way of controlling costs. Since the rise of the Net – whether Internet, intranet, extranet or whatever else is just below the horizon – new ways of doing business, providing information, and marketing products and services have arisen and raised the expectations of employees and the public for access to information.

Only a couple of years ago, people expected much less of their attempts to access information via computer systems. Now, more and more people, for various reasons, want to gain access to an organization's information systems. Access may be required, even insisted upon by the following: employees, partners, distributors, analysts, customers, or contractors, to name but a few. However, the benefit of having data on one's system is largely lost if the means and methods of access are not convenient and suitable to the business operations and the business interests of the company. If the system is vulnerable to security breaches, then value is compromised. For example, having confidential data accessible to one's competitors is one way to lose value.

Complicating this is the different work practices that many organizations are adopting. Employees may avoid commuting for an hour or more (each way) by working from home for a day or two a week. Some employees may need to work in different offices routinely, or as a part of a particular project. An increasing number of executives are out on the road – meeting clients or partners and needing to access their company's systems in order to make the best use of their time. The issue of accessibility to a company's information is one that is impacting heavily on today's businesses and the way that business is being carried out.

More and more employees make use of workgroup applications and therefore need to have common access to certain documents and data files (Leibrock, 1994). Increasingly, companies have to provide computational support to their employees who are traveling or who work remotely. It is now commonplace for branch offices which used to be self-sufficient. to access increasingly the main office systems at the company's headquarters. Where it is essential to provide 24-hour support to customers or sales agents or distributors, organizations are locating their support teams in different territories, which cover key time zones. This requires that the infrastructure of an organization must span different geographical areas, while providing for effective access, and control costs. At the same time, the need to remain in touch is growing – email and shared electronic schedulers are becoming mainstays in corporate America's life. Communication has become so easy, reliable and inexpensive that it has inspired different ways of working and doing business.

Providing remote access to a workforce raises a range of issues. Issues of security should be at the forefront of any Information Technology (IT) manager's mind. But security is a word which many people understand only superficially.

For a long time, executives in the corporate arena have recognized that it is important to manage computer installations effectively. Recently, it has also been recognized that better management of our computer systems has tended to improve their security. In order to improve computer security, organizations have to establish a policy and written doctrine, with continuous documentation, all of which spell out the security requirements and priorities and empowers the MIS department to take appropriate action to safeguard computer data. However, prior studies show that many managers felt that once they have established a policy, they have done their job (Ernst & Young, 1995, 1996, 1997). Establishing policies and not implementing and/or enforcing them nullifies their existence. Therefore, managers must possess a thorough mastery of security concepts and organizational vulnerabilities, and must develop and continuously implement enterprise-wide security policies.

Although previous studies have attempted to collect and analyze security attitude trends, no survey stands out as a benchmark of the present state of Information System Security in the academic environment. The overall objectives of this study are to determine the attitudes of IT executive candidates based on their perception of security vulnerabilities and relevant threats to the information systems of organizations and to provide a benchmark for future research on information security issues in academia.

Major changes are impacting IT, among them the Year 2000 problem, incorporating electronic commerce into the existing trading operation, the shortage of skilled IT personnel and the way Web technology will come to be used in the future. , Against this background, do those who are training to become tomorrow's information technology executives understand security issues? Do these future managers' attitudes support the implementation as well as the formation of security policies and procedures?

Overview

This research project analyzed the knowledge level and attitudes on information security issues of IT executive candidates through the administration of an attitude survey and information security tools and techniques test. The research produced recommendations to improve information security in organizations.

This dissertation begins in Chapter II with a description of the background and development of concepts of information security and then proceeds in Chapter III to look at the social aspects of technology. This is followed in Chapter IV by a description of the research methodology. Chapter V involves the analysis of the survey and knowledge data. The dissertation concludes with a discussion of the implications of this research and future research recommendations in Chapter VI, and with a summary of conclusions and recommendations in Chapter VII.

CHAPTER II

BACKGROUND AND DEVELOPMENT OF CONCEPTS OF INFORMATION SECURITY

Computer crime and other information security breaches are on the rise and the cost to U.S. corporations and government agencies is increasing. The 1998 CSI/FBI Computer Crime and Security Survey found that 64% of respondents reported computer security breaches within the last twelve months [ii]. This figure represents a 16% increase over the previous year (in which 48% of respondents reported unauthorized use) and a 22% increase over the initial 1996 survey (in which 42% acknowledged unauthorized use). Although 72% of 1998 respondents acknowledge suffering financial losses from such security breaches, only 46% were able to quantify their losses. The total financial losses for the 241 organizations that could put a dollar figure on them added up to $136,822,000. This figure represents a 36% increase in reported losses over the 1997 figure of $100,115,555 in losses (Computer Security Institute, 1998).

Security breaches detected by respondents include a diverse array of serious attacks. For example, 44% reported unauthorized access by employees, 25% reported denial of service attacks, 24% reported system penetration from the outside, 18% reported theft of proprietary information, 15% reported incidents of financial fraud, and 14% reported sabotage of data or networks (Computer Security Institute, 1998).

The most serious financial losses occurred through:

- unauthorized access by insiders

  (18 respondents reported a total of $50,565,000 in losses),
- theft of proprietary information

  (20 respondents reported a total of $33,545,000 in losses),
- telecommunications fraud

  (32 respondents reported a total of $17,256,000 in losses) and
- financial fraud

  (29 respondents reported a total of $11,239,000 in losses).

The number of organizations that cited their Internet connection as a frequent point of attack rose from 47% in 1997 to 54% in 1998. This represented a 17% increase over the initial 1996 figure of 37%. And significantly, the number of respondents citing their Internet connection as a frequent point of attack was equal to the number of respondents citing internal systems as a frequent point of attack. In the past, internal systems have been considered to cause greater security problems. It is not that the threat from inside the perimeter has diminished, it is simply that the threat from outside, via Internet connections, has increased.

CSI also reported that of those who acknowledged unauthorized use, 74% reported from one to five incidents originating outside the organization, and 70% reported from one to five incidents originating inside the organization (Computer Security Institute, 1998).

The need for increased attention to computer security has been illustrated with some high profile examples of and potentials for computer abuse that have attracted the attention of computer professionals, computer users and the public. Clifford Stoll's cuckoo's egg experience with West German hackers illustrates how easy it is to break into private computer systems, and how difficult it is to get anyone to do something about it. (Stoll, 1990) Following the cuckoo's egg incident was the Internet Worm released by a graduate student. The Internet Worm shut down between 3000 and 4000 computers for three days (Spafford, 1989) and cost government and private users approximately a $100,000,000.00 (McAfee, 1989). Over a ten-month period, a 24-year-old German Computer Science student was able to "browse" through 480 military installations in the world and successfully invade 30 of them (Hollinger, 1991).

During the past 30 years the overall business environment and the information technology embedded within it have undergone tremendous changes. (Huber, 1984). Information technology has grown by an order of in computing capacity and speed (Athey, 1988). The increasing speed and capacity of hardware technologies provide a platform for broader application of software. Personal productivity tools are now accessible throughout most organizations. New technologies on the horizon promise to improve the human computer interface, enhance the richness of electronic communication, and automate the development of more systems (Straub, 1989).

This burgeoning capability of information technology coincides with growing changes in the business environment and is exemplified by familiar business themes of the 1980s, such as mergers, leveraged buyouts, downsizing, strategic alliances, just in time scheduling, flexible manufacturing, globalization, and total quality commitment. Information Systems executives face a difficult challenge because they operate at the intersection between information technology (IT) and their organization. Information System (IS) executives must be able to interpret trends in information technology and assess its current and future impacts on their organization, while also managing day-to-day operations (Niederman, 1991).

In the context of this study, security is all about the robustness and reliability of the system, providing access in a sensible and flexible way to those who require it, and denying it to those who don't. Security also requires maintaining a log of who is doing what and the ability to access that log, receiving reports in a way that allows response in a timely manner, and preserving and protecting a company's data.

Computer security is the detection, prevention, and investigation of actual or potential acts or omissions that threaten a computer system's resources, data, or processing capabilities[iii]. Computer security includes all the problems associated with safeguarding critical resources and sensitive information in general, and also the problems that are unique to automated information processing and communications systems (Wade, 1989).

Security Concerns

The integration of executive information systems, electronic data interchange, artificial intelligence, and expert systems has propelled computing from the back office to the front lines of business operation and strategy. To remain competitive in world markets, business leaders must use the new information technology tools as an integral component in their operation and strategy. On the other hand, exposures within the information technology community have jeopardized the effective use of these systems. Computer theft through illicit hacker networks, the spread of computer virus code, computer fraud, extortion and terrorism have illustrated the increased susceptibility that accompanies the benefits in an environment of information based strategic planning, operations and communication (Fites, 1993). The emergence of computer security as a major problem has been caused by the relative success of the computer and its proliferation (Hutt, 1995).

Networks

It is not difficult to understand why computer security is poorly understood. The growth of desktop computers and workstations has outstripped that of any other technology in the corporate environment, even photocopiers. And in the future, the proliferation of networking will make this problem even more compelling [iv].

Today's desktop computers have almost as much power and memory as many corporate computer centers 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.

The importance of information security is driven by the rise in use of networks – Internet, intranet and extranets. This in turn, has led to a sharp rise in computer security incidents. The benefits from connecting an organization's computers to networks outside the organization are significant, but are accompanied by significantly increased security risks.

In less than a single life span, computer networking has shown the potential to transform organizations, communities, and the personal lives of people (Grief, 1988; Harasim, 1987; Hartmanis. 1992; Hiltz, 1993; Von Wodtke, 1993). Many Americans are incorporating computer networks into their work lives (Harasim, 1987; Rheingold, 1993). The use of these networks is becoming an essential part of modern commerce and governance (Barrett, 1989; Kiesler, 1986; Manheim, 1993; Osborne, 1992; Zuboff, 1988). The rapid adoption of computer networks has had profound consequences with regard to the change of work settings, systems of communications, and interactions with others (Boone, 1991; Hiltz, 1993; Zuboff, 1988).

Networks and information technologies provide powerful vehicles for widespread communication support to large groups of physically separated people. Computer networks create opportunities for new connections and can reduce the costs of existing communications in many business organizations (Leibrock, 1994; Sproull & Kielser, 1991).

Several studies of computer networks have discussed the increasing amount of technical innovation, the prevailing technologies, architectural developments, and commercial benefits (Chorafas & Steinman, 1990; Stewart, 1989). People tend to use networks as more than a set of peripheral tools to perform work tasks (Leibrock, 1994), and they have become increasingly intertwined (Hiltz & Turoff, 1993). The excitement of communicating with, and perhaps collaborating with, other people in networked environments became increasingly commonplace in the early 1990s (Rheingold, 1993). As network environments proliferate, people tend to rely on networks for a significant amount of interpersonal communication to coordinate work processes and to transmit messages to others in these networked organizations (Sproull & Kielser, 1993). Networked contacts among people and coordination of work have become routine in these organizations. Workers now have negative reactions to unexpected network "blackouts" and loss of communications connectivity. Employees report that they have experienced an unacceptable sense of personal isolation when confronted with network blackout situations (Raymond, 1991). To these people, network failures create changes in their everyday work routine and the temporary loss of an important business tool.

Computer networks have become an important means to remain in contact with the "home" office while traveling (Rheingold, 1993). Some people use networks from their homes not only to conduct business, but also to receive current information, including sources of news and entertainment. Individuals who use computer networks report that networks tend to alter various aspects of communications. Information contained in electronic media reportedly tends to be perceived as more accurate than voice-based information (Von Wodtke, 1993).

Organizations have become so dependent on computer based and telecommunications-intensive information systems that disruptions of either may cause outcomes ranging from inconvenience to catastrophe (Meall, 1989). Corporate risk has taken on new dimensions due to our reliance on computer and telecommunications. IT management recognized that threats to continuing operations include technological issues never before considered (Szuprowicz, 1988).

Security is often viewed as a constraint because security breaches cost money, they restrain an enterprise or because security products act as a brake on corporate goals and objectives. The reality is usually vastly different. Security is an enabling technology because it allows an organization to exploit inexpensive technological infrastructure to achieve a material benefit. If there were no security there would be no commercial potential to the Internet.

The Internet and Electronic Commerce

The Internet community spans every continent across the globe. The Internet is so large that its size is unknown, and it is evolving so quickly that its rate of growth can only be estimated. It is so diverse that it uses hundreds of different technologies, and is so decentralized that its administrators don't even know each other. The Internet is an electronic infrastructure that enables intense communications between colleagues, competitors, and disciplines. Despite these extremes, the Internet community is bound together by a framework of computer communications networking protocols and infrastructure (Howard, 1997). The Internet connects over 20 million computers in the United States and another 50 million (Denning, 1998) in 195 countries on every continent, even Antarctica (Wizards, 1998). The Internet has created a serious problem in the world of computing, criminal behavior and providing adequate security. Creating security measures that are sufficient to ensure consumer privacy is a difficult task with well over fifty million users connected through the Internet. The industry has responded, however, and is continuing in its collaborative efforts to secure the Internet. To date, the full market potential of consumer spending on the Internet has been slight at best, primarily due to the conception of insufficient security. Consumers are reluctant to punch in their credit card numbers over the Internet, specifically the World Wide Web, in fear that the arena is too wide open (Denning, 1998).

The Internet has permitted the rise of new kinds of crime that have not existed before, such as implanted viruses and breaking into computers. The Internet erases boundaries and hides jurisdictions. In recent years, hackers have gained access to credit card companies' computer systems, acquiring thousands of card numbers. Assets such as balances in users' bank accounts are one of the most common targets for computer related fraud. With more and more businesses replacing hard cash with electronically transferred transactions, the potential for abuse is great. What is often referred to as " data diddling" is hard to detect and easy to perpetrate, making the investigation of such crimes extremely difficult. Now that industry envisions a new market of expanding consumer spending over the Internet, investigation of technology to create a secure method of buying in cyberspace has begun.

Internet globalization has opened doors to criminal activities which are unprecedented, even in the most technologically-developed countries. Furthermore, high-speed telecommunications make it easier for organized criminal groups to engage in multiple activities at the same time, spreading thin the attempt by law enforcement to fight crime. Computer-related fraud has become an international security threat, but the real toll will come when such financial damage threatens the economies of developing countries. It is widely presumed that financial fraud will continue to rise, thus giving the need for security a new sense of urgency (Alexander, 1995).

Electronic commerce extends companies' reach in the marketplace and opens the door for new security problems. The advent of electronic commerce has created the most challenging environment for security technologies. The fundamental unit of activity in commerce is the exchange transaction, in which a performer delivers a product or service to the satisfaction of a customer. The customer then pays or otherwise acknowledges the performer. Authentication technologies are intrinsic to this process. Identity threat is a major concern in this arena (Wilkes, 1990). Technologies for allowing transactions to be indivisible are required. The current low-level network protocols must be redesigned to bring authentication and atomicity up to the levels required for commerce (Denning, 1998).

Security Policy

Passwords have been used for thousands of years to authenticate the identity of an individual. Passwords were the first security systems incorporated on computers 30 years ago and they represent the most common, albeit inappropriate (if used alone), security technique in today's computer environment (Klein, 1998).

A password is only one of three accepted methods of authenticating an individual to a computer. The three methods are:

1. Something known. A memorized secret word, phrase, number, code or fact known only to the user and the computer.
2. Something possessed. A discrete "token" that strongly resists counterfeiting, such as a signet ring, key or credit card.
3. Something one is. A measurable personal characteristic or "biometric," such as a fingerprint, signature, retinal pattern or voice print.

Passwords are at the heart of computer security. Requirements for a quality password are few: Passwords must be nonguessable, not in a dictionary, changed every few months, and easily remembered. User-generated passwords usually fail to meet the first three criteria, and machine-generated passwords fail the last. Several compromises exist: forcing "pass phrases" or any password that contains a special character. There are many other possibilities, but none are implemented widely. The Department of Defense recommends pronounceable machine-generated words or pass phrases (Stoll, 1990). Authorities agree that an effective computer security system requires a combination of at least two independent authenticators (Klein,1991).

Excellent programs have been developed to control user access and establish audit trails. However, these systems are worthless if the authenticated identity of the user is not guaranteed. An unsophisticated abuser can co-opt a colleague's password and not only gain unauthorized access, but also have the audit trail point to another person.

The weakest link in most computer security systems is the chosen method for identifying users. Fortunately, by implementing available "token" technologies, the threat of outsider abuse can be virtually eliminated and the threats posed by insiders substantially reduced while still retaining user convenience, network power, remote access and centralized file serving.

The range of sensitivity and value of information manipulated electronically in a commercial environment is broader than that of the information traditionally stored in filing cabinets. Information resources - including personnel, financial, marketing, and technical data - have been centralized, and broad network access, file serving, and high-density storage have become commonplace. Corporate office policies and procedures, which have evolved over the past two centuries, have been reversed, obviated, or obliterated in the last half-dozen years. For example, no responsible employee would allow a sensitive document to remain in an unattended typewriter or leave a critical engineering drawing exposed on a desk. But these same employees think little of leaving sensitive material - in even more available and exploitable form - stored in a centralized PC. As a result, the only phenomenon that has grown faster than desktop computing is corporate vulnerability (Weiss, 1990).

Cryptography

Encryption transforms a message or data files into a form that is unintelligible without special knowledge of some secret information called the decryption key. Encryption can be used as a tool to protect the confidentiality of information in messages or files. Other applications of cryptography can be used to protect the integrity of information and to authenticate its origin (Office of Technology Assessment, 1994). Many outsiders have come to believe that cryptography is the ultimate solution to computer security problems and that a new age of secure networking will dawn as soon as governments let go of attempts to regulate cryptography. However, this is a fallacy since most of the successful system attacks have exploited security weaknesses that cannot be secured by cryptography. Undoubtedly cryptography is a very important weapon in the battle of computer security; however, it is not the ultimate solution. Cryptography has allowed for the development of protocols for signing and making e-mails secret, authenticating users and servers on networks, enciphering network packets, protecting credit card numbers transmitted over the Web, and recovering lost encryption keys (Denning, 1998). Encryption technologies have created tensions over security, privacy, freedom, industry competitiveness, crime prevention, criminal investigation, public safety, and national security.

Management's Perception

Too often managers regard computer security as a technology problem rather than a management one and defer computer security to technicians (Wade, 1989). Management's perception that computer security is a technology problem stems in part from a misunderstanding. In addition to obvious technological components such as hardware and software, computer security includes both administrative issues (personnel and procedural matters) and environmental issues (physical security and hazard protection). Another point of confusion is that to many managers computer security is neither computer nor security. This opinion is formed when managers hear computer technicians disparage security as detrimental to data processing and claim that security personnel want to lock up everything indiscriminately, and when managers hear business people question the expenditure of funds and other precious resources on something so difficult to comprehend. Management tends to disregard any issue, like computer security, that lacks clear-cut organizational and staff support (Wade, 1989).

Ball and Harris found that in 1981 computer security ranked as the 14th most important information management topic (Ball, 1982). In 1985, Hartog and Herbert found that computer security had moved to fifth place (Hartog, 1986) but by 1986 it ranked in 18th place (Brancheau, 1987). A 1989 study by Neiderman found that the issue had dropped to 19th place in management importance (Niederman, 1991).

No computer security system will be effective unless corporate management is willing to initiate user education programs, establish effective policies and monitor and enforce compliance. But once policies and procedures for improved security are established, computer security falls into five areas:

1. Physical security and isolation of certain computer equipment and data media.
2. Authentication of the identity of authorized users.
3. Careful definition of user authorization.
4. Encryption of transmitted and sensitive stored information.
5. Audit trails, coupled with meaningful accountability (Hutt, 1995).

There is clearly an overlapping relationship between these areas. For example, it is meaningless to implement audit trails without reliably identifying and providing access only to authorized users. Similarly, unrestricted access to the physical computing hardware and software media render authentication and audit trails meaningless.

The technological component of computer security requires an in-depth understanding of the technology that is complicated further by the fact that computers allow voluntary actions not possible without the use of computers. The complexity of computer systems makes the consequences of voluntary actions hard to predict (Artz, 1994).

Security's fundamental objective is to reduce losses and to protect proprietary information while one of management's major focii is expanding business opportunities. Because of these differences, management often assigns computer security responsibility to the data processing department, which may seem more sensitive to management's objectives than is the security department. Finally, the fact that computer security crosses over organizational lines makes it difficult for management to identify a department that can obtain cooperation and compliance from the entire organization. This situation is another reason that management often assigns computer security responsibilities to data processing technicians because they already cross organizational lines. This management decision may be made even though there is a basic conflict of interest in allowing the unit responsible for operating the computer system also to have the final say on the type and amount of protection the system is provided.

Because it is difficult to quantify the benefits of computer security, business executives are reluctant to spend money on security. Security is seen as an overhead cost as opposed to a perceived benefit that directly adds to the bottom line. The perception is that security is a necessary evil with no perceived value. It is difficult to convince CEOs that the more reliable a system, the less confusion and the better an organization's productivity.

Poor security in an organization equates to unreliable systems, jeopardized resources, lost money, and a compromised competitive position. Although general congruence exists between how firms manage computer security and how their security officers feel computer security should be managed, some differences are apparent, particularly in the area of personnel security. Many executives feel that their firms are failing in two important areas: providing some form of security training for MIS employees and identifying employees whose particular responsibilities make them potential security risks. In addition, there are a series of minor differences between the views of security officers and the firms' practices in the area of asset-threat inventory. Most of these differences relate to either the formality of the analysis and control procedures or the importance of applying certain security programs. For the most part, the firms use subjective estimates made by people who are familiar with the assets, while security officers prefer using estimates based on the cost created if the asset were unavailable for a specified time period. Overall, security officers feel that still more can be done to enhance the level of computer security within their firms, and they recommend applying more formal analysis and control procedures to security programs, as well as increasing the frequency of certain security procedures (Makley, 1987).

Computer security is considered a "people problem," in the sense that computer security could be made more effective if employees were more aware of the need to follow certain security procedures and were trained to be on the alert for potential security loopholes (Alexander, 1995). While security managers have a general awareness of their responsibilities, they take the practical side of their job rather lightly. In some cases they have not even assessed the vulnerability of their systems (Nicolle, 1991).

The Insider Threat

The security weaknesses of both systems and networks, particularly the needless vulnerability due to sloppy systems management and administration, result in a surprising success rate for unsophisticated attacks. For all the notoriety hackers have received, insiders remain the real and persistent threat to computer systems (Landwehr, 1981). Add-on security software and hardware devices can help corporations deter computer crime, but to combat the greater problem of everyday error, security must be everybody's business.

The threat posed by hackers has doubtless helped to increase top management's interest in computer security. Nevertheless, employees' ability to access sensitive data may be potentially far more damaging than simply being able to log on to a system from outside. No matter how well formulated, all security systems are only as strong as their weakest links--human or mechanical.

The perplexing human issues of computer security must be examined so that neither employees nor outsiders can defend their actions by claiming ignorance of wrongdoing. Encouraging honesty and responsibility among employees is as important as any computer security hardware and software. The three elements that a sophisticated security program must have are clear security standards; consistent communications to let employees know these standards are in place, are important, and are enforced; and top-down leadership. Employees must understand that computer security is a principle the corporation believes in. The importance of security may be easier to get across if employees understand that not only does the corporation get hurt if its computer security is compromised, but so do its clients (Juris, 1986).

History of Computer Security

Computer security is a young field in which little research has been done to study practical applications in real life security settings (Farmer, 1996). The origins of computer security as a subject may be traced to the early 1960s when the pioneering time-sharing systems began to come into use. Users of these systems were drawn from a wide range of organizations and there was a need to prevent them from gaining unauthorized access to one another's files or, to put it more positively, to make sure any sharing of files and resources was on a controlled basis. Since everything took place in one large computer, this was a problem for the designer of the operating system (Wilkes, 1991).

There are three main aspects of information security, confidentiality, integrity, and availability. These protect against the unauthorized disclosure, modification or destruction of information (Hutt,1995).

Information security fundamentally depends on the ability to authenticate users and control access to resources. Existing user authentication mechanisms are based on information the user knows such as passwords or personal identification numbers, possession of a device such as an access token or crypto-card, or information derived from a personal characteristic -- biometrics (Denning, 1998).

Computer Security Vulnerabilities

The history of computer security failures, except for a few highly visible ones, is largely undocumented (Leveson, 1992; Spafford, 1989). Computer security flaws are any conditions or circumstances that can result in denial of service, unauthorized disclosure, unauthorized destruction of data, or unauthorized modification of data (Landwehr, 1981).

To accurately access the security of a computer system or network, one must find its vulnerabilities. This can only be done if the assessor understands the system thoroughly and recognizes the computer security flaws that threaten the system security and which can exist anywhere in the system.

A security flaw is a part of a program that can cause the system to violate its security requirements. Finding security flaws requires some knowledge of the system security requirements. This usually involves the identification and authentication of users, authorization of particular actions and accountability for actions taken (Landwehr, 1994).

Early work in computer security was based on the "penetrate and patch" process, whereby, analysts searched for security flaws and attempted to remove them. However, as soon as a flaw was discovered and corrected, more flaws always seemed to appear. (Schell, 1979).

Many organizations take a reactive versus a proactive stance regarding computer security and as a result they do not take information security seriously until a major incident has occurred. Often there is too much emphasis on the technical aspects of information security and not enough attention to the managerial aspects of information systems security (Wood, 1987). Farmer found that two thirds of the sites he surveyed had significant security problems. A third of the sites could be broken into with very little effort and approximately three fourths of all surveyed sites could be broken into if "significant force and effort were applied" (Farmer, 1996).

Computer Abuses

Beginning in the 1980s and continuing to the present day, information systems managers have cited security as a key management issue. While MIS managers are aware of the importance of information security to an organization, other managers may not be. Information from large-scale losses is often suppressed because of management embarrassment. Another complication is that management is unsure how to assess the costs and benefits of information security (Hoffer & Straub, 1989).

Hoffer and Straub also found that most organizations do not take a systematic approach to information security abuse detection. They found that only one in eight abuses were detected by security officers or auditors – 8.0%

of computer abuses were discovered by computer security officers and 4.5% were discovered by all auditors. In their study they found that most abuses were discovered by accident (32%) or by normal system controls (45%). They found that computer abuse is a serious and underreported problem. In addition, their research indicated that a large percentage of U.S. firms have experienced computer related losses and one out of five organizations experiences one or more security breaches in a three year period. Alarmingly, they also found that a single manager might be aware of less than 50 percent of the information security abuse in an organization.

On a positive note, Hoffer and Straub found that educating users on proper system security procedures and stressing penalties for misuse actually decreased levels of computer abuse. In addition they also discovered that improving detection procedures may also have a deterrent impact on computer security abuse. However, security is conceived of as a preventive function rather than as a deterrent factor.

Computer Crime

Most companies whose systems have been infiltrated do not report the incident to authorities. While this helps to keep publicity to a minimum, it prevents firms? managers? from learning from other's mistakes (Bicknell, 1995).

Security experts say that when information is stolen from a company, often the culprit is a seemingly loyal employee. Employees may steal data because of dissatisfaction with salary, promotion opportunities, or working conditions; conflict with managers; or financial problems linked to alcohol or drug use (McCollum, 1997).

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.

The world press loves to report sensational stories about hackers and cracked systems. Hacking, cracking and computer security are explosive topics at the best of times. The trend toward global connectivity and the virtual office is creating new avenues and opportunities for intruders to penetrate a company's internal network. Controlling and monitoring networks and responding to intruders are necessary to protect an organization's Internet, intranet and extranet connections (Ernst & Young, 1997).

Business Continuity Planning

Business Continuity Planning suffers from a lack of measurement standards. The drastic change in the way organizations use technology has resulted in a need for similar change in Business Continuity Planning (BCP). The changes reflect the need for a wider focus than the availability and loss of technology, and the need for a back up or contingency plan. Companies now depend on information systems to perform work that people used to do and when disasters and business interruptions occur, chaos can result (Ernst &Young, 1997).

Security Policies

The importance of information security continues to grow as managers recognize the perils of doing business in a global networked environment. Security policies and procedures, as well as trained security administrators, are the three support legs of a security architecture (Ernst & Young, 1997).

Studies of Computer Fraud, Crime and Abuse

A limited number of empirical studies have been conducted about computer fraud, crime, and abuse, computer security control and audit, and the cost of security (Straub 1990; Farmer 1996; NetVital,1998). The few studies that have been performed have not compared the way firms actually manage their computer security with the way they admit they should (Farhoomand, 1989).

In 1989, Farhoomand surveyed Fortune 500 firms to gain insight into the nature of various elements of computer security management. He found that in the area of policy direction, standards and procedures, and areas of responsibility, the surveyed firms usually have comprehensive guidelines in place. More than three-quarters of the firms have documented emergency, backup, and recovery plans. However, approximately one third of the firms never test these plans, nor do they reevaluate security programs at specified intervals.

The policies were generally formulated by consultation between the MIS manager and top management. Before computer security policies could be adopted, final approval had to be obtained from senior management. However, overall security programs were found to be weak: companies do not generally do a good job of checking up on employees once they have begun to perform their duties. In particular, firms do not:

- use attitude surveys to monitor the level of employee morale;
- consider an employee's level of security consciousness during his/her performance assessment;

- use job rotation as a means of evaluating an employee's security-related behaviors;
- use the regular vacation of a key employee to perform a mini-audit of that employee's work; and
- identify employees whose particular responsibilities make them potential security risks (Straub, 1999).

Continual security training is another weak area in the personnel security program, with 52% of firms making no provision for any form of employee security training. Slightly more than half of the firms have developed asset-threat inventories, inventories that address what safeguards protect their assets against predetermined threats. The most commonly used measures that firms employ to rank identified threats are expected loss, frequency of occurrence, hours of downtime, and dollars of damage. The remaining firms neither perform any risk assessment of security threats nor do they formally identify and evaluate their computer assets.

This chapter has discussed the technical side of information security. However, looking at the technical aspects of information security only reveals part of the picture. Any attempt to improve information security must incorporate the managerial side as well as the technical aspects. The next chapter will cover the social aspects of information technology and how it impacts on information security.

CHAPTER III

SOCIAL ASPECTS OF INFORMATION TECHNOLOGY

Any implementation of information security must be embedded within the broader mosaic of organizational change. Research suggests that culture, structure and top management's attitude are among the characteristics of an organization that affect its propensity to adopt new technology. Top management's commitment to change has a positive effect on its success (Bice, 1990; Hunsucker & Loos, 1989; Schwartz & Davis, 1981). The chief executive officer and his executive colleagues can set the tone for adopting technology as well as making the concomitant changes.

Definitions

"Socio-technical" refers to complex human-technical organizational systems where processes and technical support systems are tightly coupled. The term "socio" implies a rich mix of organizational culture and relationships.[v] A socio-technical system is a system composed of technical and social subsystems. An example of this is a factory or a hospital where people are organized in social systems such as teams or departments, to do work for which they use technical systems such as computers or x-ray machines.[vi]

Previous Research in Socio-technical Aspect of IT

A substantial body of prior research has examined the social, organizational, task, technology, and environmental factors underlying technology adoption and diffusion (Zmud, 1982, 1983, 1984; Huff and Munro, 1985; Lind and Zmud, 1990; Kwon and Zmud, 1987; Coop and Zmud, 1990; Lucas, 1975; Brancheau and Wetherbe, 1990; Robey, 1979; Davis et al., 1989; Fuerst and Cheney, 1982).

The literature on IT innovation can be examined along two major dimensions. One dimension is the unit of analysis where the research focuses on the individual as the innovator or the organization as the innovating entity. The other dimension relates to the specific factors examined as determinants of successful innovation. Several contingencies have been found to affect success or failure in the assimilation of IT.

Innovation and Implementation

Kwon and Zmud (1987) reviewed the literature on innovation and implementation in IT and identified five major forces examined in the research literature: individual factors, structural factors, technological factors, task-related factors, and environmental factors. Rather than repeat their analysis, the important point to note is that their classification provides a conceptually economic yet comprehensive basis for situating existing research.

Organizational Innovation

Other researchers have also examined organizational innovation. Gatignon and Robertson (1989) investigated the adoption of laptop computers by sales people. Even though their unit of adoption was an individual, the focus of their analysis was on the adoption decision at the organizational level. Their study included four sets of factors: the supply side competitive environment, organization and task characteristics, and decision maker information processing characteristics. Brancheau and Wetherbe (1990) tested Roger's (1983) theory of diffusion of innovation in the context of a specific information technology, spreadsheet software, with a focus on the individual as the unit of adoption. The factors they examined can be classified into individual and organizational categories.

Davis et al. (1989) examined the determinants of computer acceptance across a wide range of technologies and user populations. They postulated that perceived ease of use and perceived usefulness are the two key determinants of a behavioral intention to use computer technology. The determinants were affected by a variety of external variables such as system features and user characteristics.

Other research in technology innovation includes work that examined the assimilation process from a political perspective. In this context, Cooper and Zmud (1990) suggest that the inability to explain certain key aspects of assimilation could be caused by the political nature of the process.

Innovation Theory

Introducing technological innovation into an organization presents a complex set of challenges to management. The most complex innovations are based on information technology interacting with users in a variety of different ways and producing different outcomes, not all of which are the intended outcomes. Understanding how individuals perceive information technology issues and how these perceptions affect their adoption rates is important because it assists management to design more effective implementation strategies and offers guidance for management intervention.

Problems with user acceptance of information systems have been observed since the early days of information technology (Lucas, 1975). Despite the growing body of knowledge, these problems continue to persist (Keen, 1981; Markus, 1983) and are expected to become more pronounced (Benjamin, 1992).

The findings from implementation research suggest that the most critical problems with information technology issues are related to organization and implementation issues (Cheney, 1982; Mankin, 1984). Innovation diffusion theory recognizes that perceptions of technology do matter and are important factors influencing technology adoption. Rogers (1983) has synthesized over 1500 studies into a theory of innovation diffusion.[vii]

While the innovation studies by Rogers did not include information systems, several researchers have found his framework useful for analyzing the adoption process of information systems (Perry, 1979; Huff, 1985). Moore (1987) reviewed office automation and end-user computing literature and found the innovation diffusion model as an appropriate theoretical basis for the study and management of both types of information systems. Brancheau (1987) also considered the innovation diffusion model as the most suitable theoretical framework for information system applications because the model's focus on the individual adoption process is consistent with the degree of autonomy most knowledge workers have in carrying out their work.

Innovation Diffusion Research

The primary concern of innovation diffusion research is how innovations are adopted and why some innovations are adopted at a faster or slower rate than others. As people evaluate an innovation, they decide whether to adopt or reject the innovation. Once adopted, the decision can also be reversed at a later time. Such a decision is called discontinuance, the decision to reject an innovation once it has been previously adopted.

The rate of adoption is the relative speed with which an innovation is adopted by the members of the group. It is usually measured by the number or percentage of individuals who adopt an innovation in a specified time period. When the cumulative number of adopters is plotted over time, the result is generally an s-shaped curve. The slope of the s-curve represents the adoption rate, which may vary from innovation to innovation.

Diffusion scholars have found relative advantage to be one of the best predictors of an innovation's rate of adoption (Rogers, 1983). Tornatzky and Klein (1982) found that relative advantage, along with compatibility and complexity are the most significant factors in explaining relationships across a broad range of innovation types. Davis (1989) studied IT usefulness and ease of use, and arrived at a major conclusion that perceived usefulness is a strong correlate of user acceptance. These studies indicate a convergence of findings supporting the central role of perceived relative advantage in predicting the acceptance of information technology.

Understanding how individuals in different jobs perceive information technology, and for the purposes of this study, information security, and understanding how these perceptions and knowledge levels affect the implementation rate is important. This understanding would assist management in designing more effective implementation strategies and would offer guidance for management education and intervention.

Implementation Strategies

Most of the research on managing IT adoption and assimilation has been variance rather than process oriented (Markus & Robey, 1988). Variance or factor oriented research seeks to predict the factors that will influence a potential adopter's decision to use a particular innovation. Two dominant theories have been used for predicting IT adoption behavior, (1) Rogers' (1983) diffusion of innovations theory and (2) Davis' Technology Acceptance Model (Davis, 1989). There are many similarities between these frameworks: both identify perceived attributes of an innovation as their independent variable, and adoption behavior, or intention to adopt, as their dependent variable. Both theories apply to situations where the individual adopter can choose to adopt the innovation. The major difference is that Roger's theory identifies five perceived attributes as relevant to adoption behavior while Davis' theory identifies only two[vii]. These two theories comprise the "classical diffusion theory" research (Gallivan, 1996).

Classical diffusion studies have focused on two adoption scenarios: a scenario in which the individual end users may choose to adopt a technology or a scenario in which the organization adopts the innovation and the perceived attributes of the innovation are captured from a single adopter or decision maker. In the latter case, however, the differences of opinion or use across potential adopters in the organization are ignored (Gallivan, 1996). Most IT adoption studies utilizing classical diffusion theory have examined the adoption of PCs or personal productivity software but not individual adoption and use of complex innovations. A complex innovation is defined as an innovation with high knowledge burden or interdependencies among users.

Managerial Influence on Innovation

A major disadvantage to classical diffusion theory is that it does not consider the managerial mandates that often accompany their implementation by individuals in organizations. Such mandates are an important reality of organizational life and yet this component is not addressed by classical diffusion theory. Researchers working with variants of diffusion theory have coined numerous terms to acknowledge the existence of these mandates: managerial influence (Leonard-Barton & Deschamps, 1988), subjective norms (Davis, Bagozzi & Warshaw, 1989; Ajzen & Fishbein, 1980) or the converse, voluntariness (Moore & Benbasat). Researchers have also recognized the multi-level process through which these innovations are assimilated: a two-stage implementation process (Lucas, Ginzberg & Schultz, 1981), with separate stages of organizational and individual adoptions and primary and secondary adoption (Leonard-Barton, 1987).

Attempts to incorporate managerial influence have produced mixed results. While some studies have had success by capturing data on voluntariness to improve the explanatory power of diffusion theory (Taylor & Todd, 1995; Agarwal & Prayeshm 1995) others have not been successful (Davis, Bagozzi & Warshaw, 1989; Mathieson, 1991).

An additional limitation of classical diffusion theory is that it assumes the potential adopters decide to use an innovation when its benefits are communicated to them. This assumption, called signaling (Attewell, 1992) does not account for the steep learning curve for many innovations, such as computer security implementation techniques, which may prohibit either the initial adoption or more in-depth assimilation and diffusion into the organization. Technologies that have steep learning curves require that learning occur at the individual, the group, and the organizational level (Huber, 1991). Some researchers have argued that such organizational learning is an asset that must be built up gradually over time through developing appropriate infrastructure, absorptive capacity, and related knowledge (Cohen & Levinthal, 1990; Ross, Beath & Goodhue, 1996; Fishman & Kemerer, 1995) and cannot be acquired along with the innovation itself.

Process Frameworks

Process frameworks offer insight into how and why the chosen implementation strategy may influence the innovation's degree of acceptance or suggest why the adopter's objectives may or may not be achieved (Markus & Robey, 1988; Soh & Markus, 195). Orlikowki (1993) developed a framework to study the implementation of an innovation in two organizations. Her results emphasized the importance of managerial intentions for adopting the innovation, the actions of key decision-makers during implementation, and the broader context in which implementation occurs, in shaping the outcomes of implementation. Orlikowski found that where the intentions held by managers for the innovation represents a radical departure from the firm's existing processes or products, the employees may experience greater upheaval during implementation, compared to firms where the intentions for the innovation represent only an incremental change to the existing approach. Radical changes may lead to overt resistance and even rejection of the innovation by potential adopters. Gallivan, Hofman & Orlikowski (1994) found that if an innovation still represents a radical process change, it can still be implemented without upheaval and/or resistance if the innovation is assimilated gradually.

Agarwal, Tanniru & Wilemon (1995) propose a second process framework[viii] Their framework focuses on the distinction between the locus of adoption, which may occur at the individual or organizational level (Fichman, 1992); the difference between process and product innovations (Zmud, 1982; Orlikowski, 1993); the concepts of implementation complexity and divisibility (Leonard- Barton, 1988) as well as implementation pace (Gallivan, Hofman & Orlikowski, 1994). The Agarwal, Tanniru & Wilemon contingency framework takes the distinction between individual and organizational locus of adoption one step further, describing that both the adoption (initial use) and diffusion (widespread use) within a firm may occur at different levels of the organization. For each stage (adoption or diffusion), initiative may be taken at the individual level (through voluntary choice), or at the organizational level (through managerial mandate). Given these two dimensions: locus of adoption (individual, organizational) and stage of assimilation (adoption, diffusion), a two-by-two matrix is generated, identifying four possible innovation types, and strategies to fit them. [ix]

Three pure strategies are defined - advocacy, support and total commitment. These alternative strategies may be used alone, or in combination with each other.

The Agarwal, Tanniru & Wilemon framework integrates much of the research literature on implementing IT, and suggests that an appropriate implementation strategy depends on four variables:

1. individual adopter attributes (innovativeness);
2. the type of innovation (product or process innovation)'
3. attributes of the innovation itself (preparedness, communicability, and divisibility); and
4. the complexity or extent of the proposed implementation in the firm (implementation complexity)

In addition, the framework suggests a set of guidelines for appropriate implementation strategies, depending on the attributes listed above. On this basis, one can make *a priori* predictions about appropriate implementation strategies, and compare these to actual results.

Summary

The importance of information security may not be capturing senior executives' attention because IT managers may not be addressing security from a perspective that makes sense to those executives. The reasons for this may be because the IT managers are using language for which the senior executives have no points of reference and they may not be addressing the issues or connecting with the issues that are the focus of senior executives' attention.

CHAPTER IV

RESEARCH METHODOLOGY

Research Questions

The two research questions are:

- Do those who are being educated to become tomorrow's information technology executives understand security issues?
- Do the attitudes of these future managers support the implementation as well as the formation of security policies and procedures?

The research methodology evolved from the Ernst & Young/Information Week Information Security Survey, which has been conducted annually for the past five years. The Ernst & Young/Information Week Information Security Survey covers senior IT managers worldwide [ix]. The investigation in this study differed from the Ernst & Young/Information Week studies in that it focused on management candidate's attitudes and knowledge about information security. In addition, this study included a security knowledge component. This study evaluated the students' knowledge of information security and analyzed the following concerns: information security, network security, Internet and electronic commerce security, the needs and requirements of a business continuity plan, and security policy needs and requirements. This study was important in that it served to determine the level and depth of information security knowledge of future IT professionals, and what the attitudes and beliefs regarding development and implementation of information security are of the future IT executives.

While several surveys have been conducted throughout the years on computer security, no published survey has been administered to future IT managers, such as MBA and MPA students. Accordingly, with the consent of the Associate Dean of Technology at the College of Business Administration and the Graduate School of Business at The University of Texas at Austin, the researcher administered the instruments to two sections of such students in the Spring 1997 and Summer 1998 sections.

Research Group

The participants in the project were students enrolled in a computer security and systems audit course in the Graduate School of Business at The University of Texas at Austin. Based on prior classes, approximately 25 students were expected to enroll in each section of the course. In the supervising professor's previous experience, about 80 to 90% of the students were expected to agree to voluntarily participate in a research project of this type. [x] There were 27 students enrolled in the Spring 1997 session and 25 students enrolled in the Summer 1998 session. There were originally 52 students registered for the two sections who agreed to voluntarily participate.

Research participants were surveyed on general types of questions regarding demographics, computer usage, experience with information technology, and work experience.

The computer security and systems audit course was chosen because it was perceived to represent a set of common goals and projects with regards to computer security. Another benefit of selecting this course is that it was taught in the evening and had a high percentage of students who were experienced in the modern workplace and who expressed interest in both information technology and computer security. Most of the students demonstrated a significant mastery of personal computing skills as well as a comprehensive grasp of IT related issues. A disadvantage is that the course was only 14 weeks long, thus their longer term attitudes could not be studied. Another disadvantage of the use of this class was the element of self-selection in the sample. These students enrolled in a graduate level class in the topical area of computer audit and systems security. Most students expressed an interest in computer security. It is the researcher's opinion that the overall course structure and environment did provide a reasonable setting for testing future IT managers' attitudes about computer security.

Research Instrument

A survey instrument was designed to address the research questions listed in the introduction section. The instrument was designed after a comprehensive literature review was conducted. The security knowledge section was assembled with the assistance of Dr. Larry Leibrock, Associate Dean of Technology at The University of Texas at Austin, College of Business Administration and Graduate School of Business. The remaining five sections dealt with attitudes toward information security concerns, network security concerns, Internet and electronic commerce security concerns, the needs and requirements of a business continuity plan and security policy needs and requirements. The survey instrument was developed based on prior Ernst & Young/Information Week Information Security Surveys.

Validity and Reliability of the Instrument

Prior to being used in the study, the survey instrument was delivered to a security specialist at Cisco Corporation in San Jose, California and to an academic security expert. Both specialists were given the opportunity to critique the survey both for content and format. An interview was conducted with each specialist with an immediate response to suggestions made for the improvement of the survey. Following the suggested and implemented survey changes, the instrument was pretested to a select group of twenty graduate students, faculty and staff. These respondents were chosen from the areas of information management, accounting, marketing, management and finance. Each test respondent to whom the survey was administered was asked to make suggestions to improve the survey's readability This was done to ensure that the instrument adhered to the characteristics of attractiveness, clarity for use, and data coding (Demaline, 1979).

Null Hypotheses

In completing this study, the following six null hypotheses were tested:

Null Hypothesis 1: There is no significant difference in the knowledge of information security technologies of experienced information professionals and inexperienced information professionals.

Null Hypothesis 2: There is no significant difference in security concerns between experienced information professionals and inexperienced information professionals.

Null Hypothesis 3: There is no significant difference in network security concerns between experienced information professionals and inexperienced information professionals.

Null Hypothesis 4: There is no significant difference in Internet and electronic commerce security concerns between experienced information professionals and inexperienced information professionals.

Null Hypothesis 5: There is no significant difference in the needs and requirements of a business continuity plan between experienced information professionals and inexperienced information professionals.

Null Hypothesis 6: There is no significant difference in security policy needs and requirements between experienced information professionals and inexperienced information professionals.

Statistical Analysis

The data gathered from the surveys were keyed into a data file and imported into a statistical package for analysis, statistical manipulation and graphical depiction of the data. SPSS for Windows, version 7.5, was used for statistical processing. A description of the SPSS for Windows, version 7.5, is contained in Appendix C. Various descriptive and summary statistics for numeric variables include the following:

Central Tendency

- Mean
- Median
- Sum

- Dispersion
- Standard deviation
- Variance
- Range
- Minimum
- Maximum
- Standard Error of the Mean

Distribution

- Skewedness
- Kurtosis
- ANOVA
- Cross tabulations

Statistics and visualization methods were used for data reduction and summarization for the variable sets (Babbie 1992). All statistical charts and plots were generated with the SPSS for Windows statistical software application.

The survey results were categorized based on type of information. The data was arrayed in sets of one-dimensional enumerative tables. Actual counts and expected values were calculated.

Null Hypothesis 1 was analyzed with one-way analysis of variance (ANOVA). This procedure was chosen in order to compare the experienced with inexperienced information professionals as determined by the independent variables:

1. Years work experience
2. Classification as an Information/Audit Professional
3. Undergraduate Education
4. Graduate Program enrolled in: MBA, MPA, Ph.D, PPA
5. Major Concentration of Degree
6. Computer Proficiency (Hinkle, 1988).

Null Hypotheses 2 through 6 were analyzed with simple descriptive statistics and cross tabulations for the multiple response questions. The summary statistics focused on frequency distributions in the areas of information security concerns; network security concerns; Internet and electronic commerce security concerns; the needs and requirements of a business continuity plan; and security policy needs and requirements.

CHAPTER V

RESULTS

Overview

This chapter describes the characteristics of the 52 research participants before presenting the research findings. Participants in this research are described in terms of both general demographic attributes and personal experience with information technology. Data depicted here were obtained from the research questionnaire contained in *Appendix A: Computer Security Survey*. Following the description of the participants, the dependent variables information security concerns, network security concerns, Internet and electronic commerce security concerns; the needs and requirements of a business continuity plan; and security policy needs and requirements are described. The following independent variables were used to characterize the expertise of the users:

- Years work experience
- Classification as an Information/Audit Professional
- Undergraduate Education
- Graduate Program enrolled in: MBA, MPA, Ph.D, PPA
- Major Concentration of Degree
- Computer Proficiency

Selected statistical tests utilizing the dependent and independent variables were conducted and are discussed here. The results are arranged by the six hypotheses of the study. Details of the formal hypothesis tests are also presented in this section. Due to the number of tables produced by the statistical analysis, the tables are presented in Appendix D.

The investigation in this study differed from the Ernst & Young/Information Week studies in that it focused on students' attitudes and knowledge about information security and had a security knowledge component. The study analyzed the students' attitudes toward information security concerns, network security concerns, Internet and electronic commerce security concerns, the needs and requirements of a business continuity plan and security policy needs and requirements.

Description of the Sample

As described in the research methodology portion of this dissertation, the participants in this effort were graduate students enrolled in an elective computer security course at The University of Texas at Austin. Research participants were initially surveyed regarding general demographic characteristics, educational and professional backgrounds, computer usage, computer security knowledge, information security concerns, network security concerns, Internet and electronic commerce security concerns, the needs and requirements of a business continuity plan and security policy needs and requirements. A copy of the survey is contained in *Appendix A*. The general characteristics provide some insight to the similarities and differences of the group of students.

General Characteristics

There were a total of 52 participants in this field study. The majority of the participants were Master of Public Accounting students (68%), followed by Master of Business Administration students (36%) and one doctoral student. Not surprisingly, the majority of students' major degree concentration was in Information Management (35%) followed by Accounting (27%), Auditing (19%), with Finance, Marketing, Management completing the list. Over half (52%) the participants had Business undergraduate degrees, a fourth of the students had Engineering degrees followed by 23% with a liberal arts background.

Interestingly, 39% of the respondents had no prior work experience. A requirement of the MBA program is that students have a minimum of two years work experience prior to admission, however, the MPA program does not have this requirement which may explain the high percentage of respondents with no work experience. However, 21% of the students did have

3 to 5 years work experience, followed by 15% having 10 or more years work experience and almost 10% having 5 to 10 years work experience.

The majority of students took the course due to general interest (59%). Fifteen percent took the course because of advisor recommendation, followed by 13% due to core requirements. Eleven percent (11%) took the course because their employer recommended the course.

Almost half the participants considered themselves information or audit professionals (49%), 31% did not consider themselves Information or Audit professionals and 19% did not know if they were Information or Audit professionals.

The majority of participants (65%) did not have any prior systems of audit training, followed by 34% who had some prior systems or audit training. No participant had extensive systems or audit training.

Computer Expertise of Participants

Over half of the respondents considered themselves to have intermediate proficiency with a computer. Almost a fourth of the students considered themselves as novice computer users (23%), 21% considered themselves expert users, and only 2 students considered themselves to be technical gurus.

The majority of students, 94%, owned a computer. Only three participants did not own a computer. The majority of students used a PC Windows based computer (90%), one student used a Macintosh system and two students used both systems. The majority of participants (38%) used a computer for more than 15 hours a week, 23% used a computer 10 to 15 hours a week, 19% used a computer 5 to 10 hours a week and 1 participant used a computer for 3 to 5 hours a week. All participants used a computer at least 3 to 5 hours a week. Sixty-four percent of the students owned a desktop computer system, 25% owned both a desktop and a laptop system and 9% owned only a laptop computer system. Almost all the participants reported experience using a modem (96%).

Over half the students (58%) had published documents on the World Wide Web. The majority of students were familiar with Internet browsers, 88% with Netscape and 73% with Microsoft's Internet Explorer. Interestingly 63% had used ftp and telnet applications and half the students had used scanners and html editors. Another interesting finding was that almost twenty percent (19%) of the students had used some type of encryption tool.

The software applications most frequently used by the students were word processors (96%), spreadsheets (82%), communications software (63%), presentation software (53%) and 21% for other software. A third of the participants had written a command script, a third had not and the remaining third did not know if they had written a command script.

A large percentage of the participants, 64%, had programming experience with Visual Basic, followed by 38% with Pascal, 26% had written a C or C++ program, 17% had written programs in Cobol and Fortran, 13% in Java and 11% in CGI. Almost twenty percent (19%) had never written a computer program.

Hypothesis 1

Hypothesis 1 presented in Chapter IV was analyzed statistically for significance using the following categories as independent variables:

- Years work experience
- Classification as an Information/Audit Professional
- Undergraduate Education
- Graduate Program enrolled in: MBA, MPA, Ph.D, PPA
- Major Concentration of Degree
- Computer Proficiency

The dependent variable used to evaluate level of information security knowledge was the sum of correct answers on the security knowledge segment of the survey. There were 35 questions on various technical aspects of information security knowledge. The findings of the statistical tests are presented later in this chapter and the tables of results are in Appendix D. Hypothesis 1 was tested for significance at alpha = .05. In using the distribution tables for the identification of the critical F value, the denominator chosen was within +/- 20 degrees of freedom.

Null Hypothesis 1: There is no significant difference in the knowledge of information security technologies of experienced information professionals and inexperienced information technology management candidates.

Null Hypothesis 1 addressed the knowledge of information security technologies and implementation issues in relationship to the IT experience level of the respondents. The experience of the students was determined based upon six factors: years work experience, classification as an Information/Audit Professional, undergraduate education, graduate program, major concentration of degree and computer proficiency. Section 1 of the survey contained questions relating to the independent variables described above. A one way ANOVA table was generated that compared the independent variables to the sum of the correct answers from Section 2 – Security Knowledge of the survey. The analysis for this hypothesis appears in Table 19 in Appendix D. The analysis from the data did support the null hypothesis. Therefore, this research supports the null hypothesis that there is no significant difference in the knowledge of information security technologies between experienced and inexperienced information technology management candidates.

The ANOVA table computes the calculate f values from .594 to 1.372, therefore there were no significant differences in the security knowledge of the respondents based upon the independent variables: prior systems or audit training, computer proficiency, graduate program, information or audit professional, major area of study, undergraduate education background or work experience. Because the critical F value is greater than the computed F there is sufficient evidence to fail to reject the null hypothesis and state that there were no significant differences in the perceptions among the experienced and inexperienced IT students regarding information security knowledge.

Null Hypothesis 2: Security Concerns

Null Hypothesis 2: There is no significant difference in security concerns between experienced information professionals and inexperienced information professionals.

Null Hypothesis 2 addressed the importance of information security concerns as perceived by the experienced versus inexperienced information technology students. Section 3 of the survey instrument dealt with the attitudes toward information security concerns. The three questions in this section were taken directly from the 1997 Ernst & Young/Information Week Annual

Information Security Survey. Two of the questions requested that the respondents rank the concerns and level of threats as they perceived them in regards to information security. The results were cross-tabulated with the six independent variables: years work experience, classification as an Information/Audit Professional, undergraduate education, graduate program enrolled in, major concentration, and level of computer proficiency. An analysis of the responses to the information security concerns does not show any significant differences in security concerns based on the independent variables, therefore the data did support the null hypothesis. . The cross-tabulations and frequency tables are presented in Appendix D.

The 5th Annual Information Security Survey found that lack of human resources was the most frequently noted obstacle to effectively addressing information security risks, followed by management awareness and budget obstacles. Interestingly, the management candidates ranked the obstacles to addressing security concerns within an organization similarly. However, lack of tools/security solutions, which was ranked fourth in the Ernst & Young survey, was ranked first, followed by lack of human resources, lack of management awareness and coming in fourth, lack of budget. The comparison of the rankings are illustrated in Table 1 below.

Table 1

Obstacles in Addressing Security Concerns within an Organization

	Candidates	**E &Y**
lack of tools/security solutions	1	4
lack of human resources	2	1
lack of management awareness	3	2
lack of budget	4	3
other	5	5

However these findings are consistent with the findings by Ernst & Young where there was a disparity between the CIO and security professions relative to the adequacy of information security tools. Ernst & Young found that "information security staff are closer to the details and are more likely to have responses that differ from executives who deal with the 'bigger picture'." This finding does amplify the need for information security personnel to brief senior management on the availability and adequacy of tools.

Null Hypothesis 3: Network Security Concerns

Null Hypothesis 3: There is no significant difference in network security concerns between experienced information professionals and inexperienced information professionals.

Null Hypothesis 3 addressed the attitudes toward the need to monitor networks connections and use and importance assigned to network security issues. Section 4 of the survey instrument dealt with the attitudes toward network security concerns. The three questions in this section were taken directly from the 1997 Ernst & Young/Information Week Annual Information Security Survey. One of the questions requested the respondents rate the importance of network security issues. The results were cross-tabulated with the six independent variables: years work experience, classification as an Information/Audit Professional, undergraduate education, graduate program enrolled in, major concentration, and level of computer proficiency. An analysis of the responses to the information security concerns does not show any significant differences in network security concerns based on the independent variables, therefore the data did support the null hypothesis.

These results are consistent with the Ernst & Young findings. Just as the respondents had a low level of satisfaction with security on networks so too did the industry executives who responded to the Ernst & Young survey. Ernst & Young found that 60% of the respondents who had mission critical systems on LANs were dissatisfied with security. Ernst & Young also found that in many organizations the network connectivity issues were not well understood. This was especially true where non-IS business unit managers oversaw the installation and ongoing management of decentralized processing.

Ernst & Young found that while many organizations had successfully distributed computing power away from a central site, decentralization of security administration had been a disappointment. They attributed the disappointment with decentralized security administration to the following factors:

- Decentralized security administration was often a part-time responsibility, which was viewed as largely clerical in nature.
- No training for decentralized security administrators.
- Security responsibilities were not included in job descriptions, performance evaluations, or incentive bonus criteria for decentralized administrators.
- A lack of centralized monitoring and enforcement of policy and standards resulting from an oversight of the decentralized processes.
- A lack of guidelines assisting remote administrators in selecting the proper security for new technology platforms or application software packages.

Ernst & Young concluded that in a distributed computing environment, security cannot remain fully centralized and be responsive (Ernst & Young, 1997). This appears to also be the attitudes of the management candidates in that their responses mirror the responses received by Ernst & Young.

Null Hypothesis 4: Internet and Electronic Commerce Security

Null Hypothesis 4: There is no significant difference in Internet and electronic commerce security concerns between experienced information professionals and inexperienced information professionals.

Null Hypothesis 4 evaluated the satisfaction with Internet security, the attitude towards control techniques for Internet and electronic commerce, and the media used for electronic commerce. The four questions in this section were taken directly from the 1997 Ernst & Young/Information Week Annual Information Security Survey. The results were cross-tabulated with the six independent variables: years work experience, classification as an Information/Audit Professional, undergraduate education, graduate program enrolled in, major concentration, and level of computer proficiency. An analysis of the responses to the information security concerns does not show any significant differences in security concerns based on the independent variables, therefore the data did support the null hypothesis.

Forty-eight percent of the respondents were not satisfied with the overall level of security of their connection to the Internet. Ernst & Young found that 34.8% of management was not satisfied with the overall level of security of their connection to the Internet. However, this was an improvement from the previous year's findings where 40% were not satisfied. Comparison of findings between the Ernst & Young respondents and the students is interesting in that the majority of management was satisfied with the overall level of security in Internet connectivity and almost half of the students, 48%, were not satisfied with the level of security. Another interesting fact is that 32% of the students had no opinion about the level of security whereas all the executives polled had an opinion.

Table 2

Satisfaction with Overall Level of Security of Connection to Internet

	Candidates	E & Y
Yes	20%	65%
No	48%	35%

There was also a wide variation in the ranking of actual control techniques used by industry and the prioritizing of control techniques that the management candidates would use for electronic commerce. The variation is listed below in Table 3. While passwords were rated as the most frequently used method by industry, the management candidates rated them as third. However, there was agreement between the two groups regarding the second most commonly used control technique, trading partner identification and profile verification, as well as agreement on the sixth ranking, application acknowledgements.

Table 3

Ranking of Control Techniques Used for Electronic Commerce

	Candidates	E & Y
Message authentication codes	1	7
Trading partner ID and profile verification	2	18
Passwords	3	1
Encryption	4	5
Functional acknowledgements	5	8
Application acknowledgements	6	6
Control totals	7	4
No control techniques needed	8	3

Another deviation from the Ernst & Young findings occurred in the type of media used for electronic commerce. Table 4 below illustrates the different rankings.

Table 4

Media Used for Electronic Commerce

	Candidates	E & Y
Internet	1	5
Dialup	2	3
Leased Line	3	2
Intranet	4	6
Magnetic media	5	2
Other	6	4

The most commonly used media for electronic commerce by business executives was magnetic media, as opposed to the most commonly used medium by candidates, the Internet. This could possibly be the result of the different type of resources available to the two different groups.

Null Hypothesis 5: Business Continuity Plan

Null Hypothesis 5: There is no significant difference in the needs and requirements of a business continuity plan between experienced information professionals and inexperienced information professionals.

Null Hypothesis 5 addressed the necessity and requirements for a business continuity plan within an organization. Section 6 of the survey contained two questions about the need for and what should be contained in a business continuity plan. The questions in this section were taken directly from the 1997 Ernst & Young/Information Week Annual Information Security Survey. One of the questions requested that the respondents select what should be included in the plan . The results were cross-tabulated with the six independent variables: years work experience, classification as an Information/Audit Professional, undergraduate education, graduate program enrolled in, major concentration, and level of computer proficiency. An analysis of the responses to the information security concerns does not show any significant differences in security concerns based on the independent variables, therefore the data did support the null hypothesis. The cross-tabulations and frequency tables are presented in Appendix D. Interestingly, all of the respondents believed that a business continuity plan is important.

Likewise, three-quarters of the respondents to the Ernst & Young survey had a business continuity plan. Interestingly while 75% of the Ernst & Young respondents had a formal corporate information security policy only 38% indicated their organizations had an information security orientation of new employees and only 48% had an ongoing information security awareness program of periodic communication to employees. These statistics did not change measurably from the prior years' studies. Ernst & Young concluded that either management believed that training and strengthening of general security awareness was not critical or that a lack of resources did not allow such training. Alternatively they concluded that organizations may believe that security awareness training was not necessary.

Null Hypothesis 6: Security Policy

Null Hypothesis 6: There is no significant difference in security policy needs and requirements between experienced information professionals and inexperienced information professionals.

Null Hypothesis 6 addressed the needs and the requirements for an information security policy as perceived by the experienced versus inexperienced information technology students. The last section of the survey instrument dealt with information security policy needs and requirements. The six questions in this section were taken directly from the 1997 Ernst & Young/Information Week Annual Information Security Survey. One of the questions requested that the respondents rank the importance for senior management involvement in information and data security. The responses to the six questions were cross-tabulated with the six independent variables: years work experience, classification as an Information/Audit Professional, undergraduate education, graduate program enrolled in, major concentration, and level of computer proficiency. An analysis of the responses to the information security concerns does not show any significant differences in security concerns based on the independent variables, therefore the data did support the null hypothesis.

The findings from this section also correspond with the Ernst & Young findings. Ernst & Young found that the importance of information security continued to increase as managers began to recognize the perils of doing business in a global networked environment. Security policies, procedures, and trained security administrators are the three support legs of a security architecture. Ninety-two percent of candidates felt that an organization needed a stand alone information policy, Ernst & Young found that 80% of their respondents has a stand alone policy, however 20% had not created security policies.

The implication of the results of the six hypotheses will be discussed in the following chapters. Chapter VI will discuss the policy implications and future research recommendations. Chapter VII will summarize the study and its conclusions.

CHAPTER VI

IMPLICATIONS AND FUTURE RESEARCH RECOMMENDATIONS

This chapter presents policy implications of this research and recommended actions for information technology companies and business schools to improve information security. This chapter also presents an analysis of the current state of information security in the workplace and academia and recommends modifications to the existing policies and procedures.

While several studies have been conducted on information security, there appears to have been no definitive study of information security knowledge and attitudes of information technology management candidates. In order to explore this issue, this study employed the following:

- An information security knowledge test;
- A multi-section survey based upon an annual survey administered to IT professionals; and
- An extensive data analysis of an information security attitude survey and security knowledge test administered to information technology management candidates.

The research was intended to help evaluate the security knowledge and information security perceptions of information technology management candidates. In addition, this study was developed to help provide information on information security needs which may aid in the effective design of future information security courses. The course selected as a testing ground appears to have been an appropriate test sample since the students enrolled in the course stated an intention to work in the information technology field and aspire to IT executive status.

The research present in this dissertation is not to be considered at its final terminus. Much research is needed to properly underpin and validate the continued practicality of the concepts set forth above. This study was a departure from many of the prior studies done on information security since it was designed to test the knowledge and attitudes of future IT executives. A more widespread study is needed to further test the hypotheses of this study. One technique that may yield more conclusive results would be a pre and post cohort analysis which would require a larger sample size than the present study. Further studies are planned for the coming year and the study will be extended to include a range of information technology programs and schools.

In future research, it might be instructive too explore the ways in which the specifics of the respondents professional experience and business environment influence their responses. A possible option would be to examine if there are any differences which correlates to their professional experience.

This could be further broken down into businesses that have an electronic commerce component and perhaps further explore the differences that might appear based on the degree of involvement in electronic commerce and the business tasks which are carried out via electronic commerce. An example would be to see if it were possible to differentiate between respondents who organizations use electronic commerce in a business to business and/or consumer to business context.

Clearly the results of this study indicate that there is a strong need to educate students enrolled in information technology programs about the technical aspects of information security. While all of the graduate students in this study had similar concerns and had similar beliefs about the importance of information security, prior experience with Information Technology was not indicative of information security knowledge regarding the techniques and concepts of information security.

Education on computer security is poor. Many, if not most information networks are operating with nonexistent security policies. Lack of awareness is pervasive. Education is the single most important aspect of security (Anonymous 1997). If we are to address effectively the issues raised as a result of the widespread use of technology we must make information security a priority instead of an afterthought. In addition, the education of our future managers must include an information security component. The focus on computer security can be achieved through an alignment of the security domain among business, government and education. It is imperative that business take a proactive role in information security education. At the same time, education should begin as early as kindergarten and continue through postsecondary education regarding the importance of personal and ethical responsibility when using computers. There needs to be an emphasis on the role of information security that begins as soon as computers are introduced to children in the educational system, even as early as the kindergarten level.

Studies show that information security continues to be ignored by top managers, middle managers, and employees alike. The result of this unfortunate neglect is that organizational systems are far less secure than they might otherwise be and that security breaches are far more frequent and damaging than is necessary. The underlying problem is that many managers are not well versed on the nature of systems risk, likely leading to inadequately protected systems.

Organizational information systems today remain in jeopardy. Over the years, study after study has documented actual and potential systems losses (Parker, 1976; 1981; 1983; Hoffer and Straub, 1989; Loch, Carr, and Warkentin, 1992). A partial listing of institutional sponsors of high profile studies includes: the U.S. Government (Kusserow, 1983; Colton, Tien,, Davis, Dunn and Barnett (1982a, 1982b), the American Bar Association (1984), the American Institute of Certified Public Accountants (1984), Ernst and Young (Burger, 1993), and Ernst & Young (Panettieri, 1995), and, abroad, the Local Government Audit Inspectorate (1981). Estimates of annual losses vary, but some set losses at between $500 million and $5 billion per year in the U.S. alone (Flanagan and McMenamin, 1992). If anything, losses have become even more serious as time goes on (Schwartz, 1990).

Yet, in spite of voluminous evidence that systems risk is high and that many organizations are under-secured, many managers continue to ignore the issue and to be "naive" in their responses to the challenge posed by this growing threat (Loch et al., 1992, p. 183). Why is this so? One viable explanation is that systems risk has been a back-burner issue for decades, even among managers who specialize in information technology (IT), and it is difficult to change a perception with such momentum. Tellingly, although IT executives have included systems security in their list of critical issues (Ball and Harris, 1982; Dickson et al., 1984; Hartlog and Herbert, 1986; Brancheau and Wetherbe, 1987; Niederman, Brancheau, and Wetherbe, 1991), only once have they ranked it among the top ten issues. Even more tellingly, both "disaster recovery" and "security and control" dropped off the top twenty ranking in the latest key issues study (Brancheau, Janz, and Wetherbe, 1996).

If managerial perception of systems risk is lower than it should be, why is this the case? How does a manager develop a sense that his or her risk-cost tradeoff is well balanced? While a few studies have addressed this issue conceptually, one study has explored the issue from both a theoretical and empirical perspective (Goodhue and Straub, 1991). These authors argue that managerial concern about the organization's security is a function of: (1) risk inherent in the industry, (2) the extent of the effort already taken to control these risks, and (3) individual factors such as awareness of previous systems violations, background in systems work, etc. Independent colloboration of these factors has been reported by Dixon, Marston, and Collier (1992).

How can managers' consciousness about security risk be heightened? If this model is accurate, then clearly it is necessary to alter managers' perceptions of the three underlying components of risk in order to affect their overall perception of risk. Education about information security must become a priority in education at all levels, beginning with K-12 and continuing beyond the graduate level into the workplace. In addition to incorporating information security into the curriculum there needs to be a push for executive education.

For years, the received wisdom of security experts is that countermeasures, strategies that are adopted to reduce systems risk, fall into four distinct, sequential activities, namely: (1) deterrence, (2) prevention, (3) detection, and (4) recovery (Parker, 1981; Martin, 1973; Forcht, 1994). Not surprisingly, perhaps, these four classes of sequential actions have a strong theoretical basis.

The theory that best explains the effectiveness of these countermeasures is general deterrence theory. Used in the study of criminals and other anti-social personalities, the theory is well established in criminology (Blumstein, 1978; Pearson and Weiner, 1985). It posits that individuals with an instrumental intent to commit anti-social acts can be dissuaded by the administration of strong disincentives and sanctions relevant to these acts. In more easily understood terms, active and visible policing is thought to lower computer abuse by convincing potential abusers that there is too high probability of getting caught and punished severely.

General deterrence theory has been applied successfully to the IS environment by Straub and his research partners (Straub, Carlson, and Jones, 1994; Straub, 1990; Straub and Nance, 1990; Hoffer and Straub, 1989). The basic argument in this work is that information security actions can deter potential computer abusers from committing acts that implicitly or explicitly violate organizational policy. Moreover, they have found empirical evidence that security actions can lower systems risk. Specific application of general deterrence theory to information security is based on the underlying relationship between activities of managers and that of computer abusers (Nance and Straub, 1988).With respect to risk from computer abuse, this model asserts that managers are themselves the key to successfully deterring, preventing, and detecting abuse as well as pursuing remedies and/or punishing offenders for abuse.

Straub and Welke (1999) found that a certain portion of potential system abuse is allayed by deterrent techniques, such as policies and guidelines for proper system use and by reminders to users to change their passwords. Deterrent countermeasures tend to be passive in that they have no inherent provision for enforcement. They depend wholly on the willingness of system users to comply. Security awareness programs are a form of deterrent countermeasure which deserve special mention here because educating users as well as their superiors about security yields major benefits. These sessions convey knowledge about risks in the organizational environment; emphasize actions taken by the firm, including policies and sanctions for violations; and reveal threats to local systems and their vulnerability to attack. A major reason for initiating this training, however, is to convince potential abusers that the company is serious about securing its systems and will not treat intentional breaches of this security lightly. In essence, potent security awareness training stresses the two central tenets of general deterrence theory — certainty of sanctioning and severity of sanctioning (Blumstein, 1978).

Current thinking and practice were also lacking an effective mechanism to evaluate the fit between business needs and potential solutions. At present, the literature advocates only a crude cost-benefit mechanism that falls far short of the kind of intellectual tools that would lead to high quality, scientific assessment and good planning decisions (Baskerville, 1991). The problem with such present first generation tools (Baskerville, 1993) is that they are atheoretical (Hoffman, 1989). As simple heuristics that estimate rough-cut costs of an unsecured system and the benefits of implementing security controls, they play down or completely ignore the behavioral side of the phenomenon of computer abuse. Present atheoretical techniques are also incapable of evaluating the synergy offered by combinations or sets of security controls. In fact, practitioner and academic interest in information security (IS) planning has been marginal. Planning for security is mentioned only briefly in this literature (viz., McLean and Soden, 1978; Steiner, 1979, 1982; King, 1984; Venkatraman, 1985-86; Ramanujam and Venkatraman, 1987; Lederer and

Sethi, 1991). These studies neither detail the nature of security planning nor the process stages required for a successful planning effort.

Likewise in the more specialized security and control literature, the issue of security planning has not been dealt with. Although Parker (1981; 1983), Fisher (1984), Caroll (1987), Baskerville (1988; 1993), and Forcht (1994) all discuss means by which threats to systems can be identified and countermeasures proposed, they do not discuss this process as a planning process per se. (does per se need to be italicized?) Stages in a normative planning process are not articulated in the literature nor are the desired outcomes of the stages.

Baskerville (1993) argues that planning for security should ideally be incorporated in systems development, and security controls designed at the logical systems level, in parallel with actual system functionality. Recognizing that systems projects seldom unfold in this fashion, Baskerville goes on to argue that ex post security enhancement can indeed be undertaken for existing and legacy systems.

Other than Baskerville (1993), the scholarly and consulting literatures on security do not provide a commonly agreed upon conceptual model for the security planning process. Much of the literature, indeed, specifies in detail only one of the central activities of the process, namely, risk analysis (Parker, 1981, 1983; Fisher, 1984; Caroll, 1987; Badenhorst and Elof, 1989; Eloff, Labuschagne, and Badenhorst, 1993). Whereas von Solms, van de Haar, von Solms, and Caelli (1994), de Konig (1995), and others discuss various types of planning (e.g., disaster recovery planning vis-à-vis contingency planning vis-à-vis physical security planning, etc.), there is little in the public domain describing an overall approach to security planning and evaluation or the specific details of this process.

Developing effective information security policies and procedures requires that decision makers have a certain level of awareness of industry standards for security. An effective way of achieving this is through security awareness training, or the training of managers and other professionals in proper use of system assets. In this training, security specialists review with employees policies (if they exist), system authorizations, conditionalities for use, methods for changing passwords, penalties for security breaches, and other topics that have a bearing on preventing misuse of system assets. The training should also make participants aware of the general effectiveness of deterrent, preventive, detective, and remedial countermeasures in lowering systems risk.

As Straub and Welke (1999) point out forward-looking and proactive security programs are exceptional in most industries. Fewer than half of organizations are likely to have active security awareness programs in place; moreover, about two thirds believe that information security is not a significant issue (Kearns, 1994). Such views fly in the face of commissioned studies that have consistently concluded otherwise (Kusserow, 1984; American Bar Association, 1983; Dixon, et al., 1992).

Straub and Welke found that managers tended to see computer security as a way to prevent losses and thereby mitigate further downstream damage. Much less frequently were they concerned about how to recover from a security breach or system loss and seek remedies. Moreover, managers were seldom attuned to deterrents as a tool for reducing system risk. They were even less aware of the value of systematic and purposeful detection. Very few participants demonstrated an awareness of the feedback effect of countermeasures.

Given that the present study examined management candidates' attitudes and knowledge about information security, researchers may want to test the generalizability of these findings. Researchers should investigate the effect over time of education of both existing management and management candidates. It is possible that even once awareness is raised, management may lose the orientation and revert back to atheoretical approaches in addressing security issues. Researchers may also want to investigate the viability of theory-based security planning since little scientific work has been done in this area (Straub and Welke, 1999).

The final chapter will expand on the issues raised by this study and will set forth recommendations for academia and industry on how to address the lack of information security knowledge that exists in the information technology field.

CHAPTER VII

SUMMARY AND CONCLUSIONS

Often there is too much emphasis on the technical aspects of information security and not enough attention to its managerial aspects (Wood 1987). Farmer found that two thirds of the sites he surveyed had significant security problems. A third of the sites could be broken into with very little effort and approximately three fourths of all surveyed sites could be broken into if "significant force and effort were applied" (1996).

On the other hand, Hoffer and Straub (1989) found that educating users on proper system security procedures and stressing penalties for misuse actually decreased levels of computer abuse. In addition, they also discovered that improving detection procedures may also have a deterrent impact on computer security abuse. However, security was considered to be a preventive function rather than as a deterrent factor.

Summary

Two research questions were formulated from an in-depth literature review and preceded the development of the survey instrument. This survey instrument was administered to two sections of a computer security and audit course taught in the Graduate School of Business at The University of Texas at Austin during the Spring and Summer of 1998. Respondents were surveyed about their information security knowledge and their attitudes and perceptions regarding the following topics: (1) information security concerns; (2) network security issues; (3) Internet and electronic commerce information security issues; (4) needs and requirements for a business continuity plan; and (5) security policy requirements. The data were analyzed with the SPSS statistical software package, version 7.5 for Windows. Data comparing security knowledge and attitudes with the following six independent variables was analyzed: (1) years of work experience; (2) classification as an Information or Audit Professional; (3) undergraduate education; (4) graduate program enrolled in; (5) major concentration of degree; and (6) computer proficiency were analyzed with an ANOVA test and frequency and descriptive statistics were employed. Data comparing groups for Hypotheses 2 through 6 were analyzed by means of frequency distributions, descriptive statistics and multi-response cross tabulations, in order to discover if there were any significant differences in security knowledge and attitudes based upon the six independent variables.

Conclusions

The conclusions of the study are reported as they relate to the research questions as outlined in Chapter I and IV. These are based on the statistical analysis results reported in Chapter V.

Research Questions

The research questions for this study were:

- Do those who are training to become tomorrow's information technology executives understand security issues?
- Do these future managers' attitudes support the implementation as well as the formation of a security policies and procedures?

Discussion of Null Hypothesis 1

Null Hypothesis 1: There is no significant difference in the knowledge of information security technologies of experienced information professionals and inexperienced information professionals.

Based upon the sum of correct answers to the information security knowledge component of the survey there was no statistical difference in the knowledge of students who were experienced in Information Technology and those that were not. This illustrates the need for information security education to be incorporated into graduate business education programs

Discussion of Null Hypothesis 2

Null Hypothesis 2: There is no significant difference in security concerns between experienced information professionals and inexperienced information professionals. There were no significant differences in security concerns between of students who had experience in Information Technology and those that were not. All of the students were concerned about the threat of unauthorized information being disclosed and had concerns about the security of information/data.

Discussion of Null Hypothesis 3

Null Hypothesis 3: There is no significant difference in network security concerns between experienced information professionals and inexperienced information professionals.

Again, there were no statistical differences in network security concerns between experienced information technology students and inexperienced students. All of the students felt that an organization should monitor network connections with trusted business partners and that an organization's LANs and WANs should be actively monitored.

Discussion of Null Hypothesis 4

Null Hypothesis 4: There is no significant difference in Internet and electronic commerce security concerns between experienced information professionals and inexperienced information professionals.

There were no statistical difference between groups in regard to Internet and electronic commerce concerns. All students felt that control techniques were needed for electronic commerce business transactions and Internet connections.

Discussion of Null Hypothesis 5

Null Hypothesis 5: There is no significant difference in the perception of the need and requirements for a business continuity plan between experienced information professionals and inexperienced information professionals.

There was no significant difference between groups regarding the need and requirements for a business continuity plan. All respondents felt that a business continuity plan was needed by organizations.

Discussion of Null Hypothesis 6

Null Hypothesis 6: There is no significant difference in perception of security policy needs and requirements between experienced information professionals and inexperienced information professionals.

Lastly, there was no significant difference regarding the perception of need and requirements for a security policy between groups. All students felt that a security policy was needed and that an organization should implement security measures on their systems and information.

This research has been an attempt to determine if a difference exists between attitudes toward information security between information technology managers and candidates for information technology management positions. It has also been an attempt to determine the degree of information security knowledge that graduate students of information technology possess.

Recommendations

The Internet is being transformed from a medium for distributing multimedia data to a medium for conducting business. The Internet is a major player in business because it enables businesses to do deals with people anytime, anywhere. The explosion in the size of the Internet in recent years can be directly tied to the prospect of performing business online (Denning, 1998). However, this growth has resulted in an increased need for and increased importance of information security. The original Internet was designed for research, not as a commercial environment. As such, it operated in a single domain of trust.Provisions were made to allow remote users to access critical files on machines through the use of BSD r (UNIX) commands (e.g., rlogin and rsh), and security relied on users' mutual respect and honor, as well as their knowledge of conduct considered appropriate on the network. Minor security was made available in the form of password-protected hosts but was basically an afterthought in design.

As the Internet grew, the community expanded, and the existing security framework was found to be inadequate. This has been demonstrated in the past few years in the form of Internet-based attacks on commercial systems:

- The Morris Worm of 1988 (Eichin & Rochlis, 1989);
- The "Berferd" incident at AT&T in 1991 (Cheswick, 1991);
- The theft of passwords from service providers in late 1993 and early 1994;
- The "IP Spoofing" attack on the San Diego Supercomputer Center in late 1994 (Shimomura, 1996); and
- The theft of funds from Citibank in 1995.

For the most part, these attacks took advantage of simple holes largely attributed to misconfigured systems, poorly written software, mismanaged systems, or user neglect. The continuing evolution of our technological base and our increasing reliance on computers for critical tasks suggests that future attacks may well have more serious consequences than the ones that have occurred.

Recommendations for Academic Programs in Information Technology

In today's heavily internetworked computing environment, it is imperative that managers and students of information management have an understanding of information security principles and practices. On the academic side, an ever growing number of colleges and universities have introduced courses in computer security. While this increased attention to security in academia is a good sign, the courses are generally offered as electives (Denning, 1998). As an elective course, a significant number of students will not have the opportunity to take the course, which means that a significant number of information management candidates will graduate without a solid background and basic understanding of security. In addition waiting until college level is insufficient. Information security education needs to be introduced with the initial introduction to computers. Ensuring that individuals who obtain information technology degrees have a sound foundation in security principles is becoming increasingly important as the worldwide connectivity of our networks grows and a corresponding rise in the number of security incidences occurs. Increasing the number of courses professional information management students are required to take by adding additional courses dealing with security is one option for ensuring that a sound foundation is obtained. Another, possibly more realistic approach, is an organized approach to include security topics into already existing curricula (as was first proposed in ACM's Curricula '91 document). This approach entails going beyond briefly mentioning security at various points, instead it advocates pioneering the concept of using security to actually teach core information technology principles.

The ACM Curricula '91 document proposed that a basic number of computer security and ethics courses be covered in all information technology programs. While the option to offer an elective course was acknowledged, the document proposed that a certain number topics be covered at appropriate times in the curriculum. This passive approach to security education is not enough. At the same time, information management programs do not have the luxury of adding additional required courses to their already full program.

The solution is to introduce an organized approach to teaching security across the curriculum. Instead of addressing security topics as separate issues, security should be woven into all courses that make up the fabric of the core information management curriculum. The introduction of information security across the curriculum should not come at the expense of other topics. In certain courses, because of their very nature, security can be used to teach the course itself. Any incorporation of information security modules across the curriculum should begin with the first introductory computer course. In addition there needs to be a complementary introduction of computing responsibility and ethics when computers are introduced to students even as young as kindergarten age. At this basic level the detail required is minimal. Exposure to the concept of viruses and how to protect against them, good password management techniques, and elementary encryption issues would serve to introduce the student to the idea that security should be a concern.

An operating systems course provides many opportunities to address security issues both from a practical and a design point of view. Issues such as access control are already part of many textbooks on operating systems. Other issues such as authentication, object reuse, auditing, and security kernels would also integrate well at this level.

While entire books have been written on database security, many textbooks designed for introductory database courses often spend only a few pages on the subject or ignore it completely. Issues such as multilevel protection, polyinstantiation, access modes, auditing, and inference controls need to be incorporated into every database course. Additionally, a networks course is another good course to incorporate a security component. There are numerous security topics which can be used to illustrate or emphasize various network principles. Among these are cryptography, intrusion detection, firewalls, "worms", and security among distributed systems.

Software engineering courses, with their emphasis on the entire life cycle of software, also present several opportunities to discuss security issues. The design phase of software development provides the chance to discuss the modeling of secure systems. Discussion of program testing provides similar opportunities to discuss verification and validation. Covert channel analysis can also be easily introduced into the course.

Recommendations for Management Education

It is never possible to achieve 100% security. Systems are too complex. Humans make mistakes. Unanticipated events arise. New technology arrives before its security implications are fully understood. Vendors rush products to market in response to customer demand. Moreover, with security comes tradeoffs with flexibility, openness, ease of use, performance, and interoperability, and so security must be balanced with these other objectives.

To be effective, security must be integrated into the design, implementation and operation of an entire operating environment: from the lowest-level programs, to the applications, to the procedures and practices. This can only be accomplished if all levels of management are aware of the security concerns. Good information security can help good management but no amount of it can compensate for bad management. Information security is a management problem and a technology problem. If systems are riddled with security flaws, there is little incentive to use serious user authentication. Management's options are limited thereby. In addition, there are issues with respect to which security is also a user problem, an education problem, and a legal problem.

The current trend toward open systems, client-server computing, and the blending of computing with communications should make management focus on the trade-offs in balancing adequate IT protection with end-user productivity and the expenses of administering and auditing security across a wide variety of computer systems. Management needs to reexamine the business goals of IT security within their organizations.

Managers must recognize that security is important to their success because it is fundamental to the accuracy and reliability of the IT systems that support their objectives of internal cost reduction, rightsizing, and customer service. IT security is the only way management can automatically enforce their policy decisions on the computer systems for which they are responsible. The shift in the importance of information technology to a position of prominence with regards to the survival of the organization may have escaped the notice of management (Baskerville, 1988). Most of the work in computer security has taken a very technical perspective. Even when people are considered with respect to security, the view has been more instrumental than beneficial. A fundamental element of the problem is the narrow view held by many managers, analysts and designers, that the security problem is wholly a computer problem. Attempts to secure modern information systems applications such as office automation or decision support systems purely through computer security are misguided.

The key to successful information security is for management and technologists to realize that information security requires the commitment and involvement of all levels of an organization: upper management, technology management, users, those providing education and providers of legal analysis. Dealing with only one of these elements will result in the continuance of the poor information security practices that now exist. To be successful, information security efforts must incorporate all of these aspects of an organization, whether business organization or academic institution.

ENDNOTES

[i] The literature on modern organizations contains many references to the importance of information technology. The following authors include discussions on information technology: Chorafas (1990) Cleveland (1985), Galbraith (1973); Flamm (1989), Harmon (1993), Hartmanis (1992), Nonake (1991), Porter (1990), Quinn (1992), Sakaiya (1991), Senge (1990), Stalk (1990), Thurow (1992).

[ii] Established in 1974, the Computer Security Institute is the oldest international membership organization offering training specifically targeted to information security professionals. The Institute's primary purpose is to provide education on practical, cost-effective ways to protect an organization's information assets. CSI is the industry leader in skills-oriented training for information security practitioners.

[iii] As is the trend in current literature, the use of terms information security and computer security the terms are used interchangeably in this dissertation.

[iv] The term *computer networks* and *networks* in this context includes the information technology, software, tools, machinery, knowledge, content, and the social and cultural context within which these networks are employed.

For the purposed of this research the terms *information technology* and *computer networks* are used synonymously.

[v] Taken from the research by Dr. Jason Scholz, downloadable from http://www.itr.unisa.edu.au/~dstowww/socio-technical/welcome.htm.

[vi] Excerpted from two reports by Dr. Bernd Hornung and based on a list of definitions concerning evaluation and technology assessment in English. There is a more substantial list concerning also system and management directly in German, which would need to be translated.

[vii] Rogers (1983) identifies five perceptual characteristics of innovations which help explain differences in adoption rates: relative advantage, compatibility, complexity, trialability, and observability. These are defined as follows:

> Relative advantage - the degree to which an innovation is perceived as better than the idea it supersedes. Compatibility - the degree to which an innovation is perceived as being consistent with the existing values, past experiences, and needs of potential adopters. Complexity - the degree to which an innovation is perceived as difficult to understand and use. Trialability - the degree to which an innovation may be experimented with on a limited basis. Observability - the degree to which the results of an innovation are visible to others. Typically, the

> rate of adoption is positively related to perceived relative advantage, compatibility, trialability, and observability and is negatively related to perceived complexity of the innovation.

Rogers defines diffusion as "the process by which an innovation is communicated through certain channels over time among the members of a social system." He defines innovation as "an idea, practice or object that is perceived as new by an individual or other unit of adoption."

[viii] The Agarwal, Tanniru & Wilemon matrix and the implementation strategies are illustrated in Appendix C.

[ix] Ernst & Young LLP has conducted an annual Information Security Survey since 1992. The surveys and results can be downloaded in Adobe Acrobat format at http://www.ey.com/publicate/tce/

[x] Dr. Larry R. Leibrock has taught this course for the past 3 years in the Graduate School of Business at The University of Texas at Austin. His estimate was based on previous research efforts at The University of Texas.

APPENDIX A: INFORMATION SECURITY SURVEY

Part 1: Demographics

1. Why did you elect to take this course:

1. General interest
2. Recommendation from advisor
3. Recommendation from employer
4. Fulfill course requirements
5. No particular reason

2. Do you consider yourself an information or audit professional?

1. Yes
2. No
3. Do not know

3. What is the extent of your prior systems security or systems auditing training:

1. Extensive
2. Some
3. None

4. Undergraduate Education:

1. Liberal Arts
2. Business
3. Engineering/Sciences
4. Other

____

5. Are you presently enrolled full time in graduate school?

1. Yes
2. No

6. What graduate program are you enrolled in

1. MBA
2. Ph.D area:__________________
3. Masters area__________________

7. What is the major concentration of your degree

1. Information Management
2. Audit
3. Finance
4. Accounting
5. Marketing
6. Management
7. Other ______________________
8. None

8. Previous Graduate Education:

1. Graduate Liberal Arts
2. Graduate Business
3. Graduate Engineering/Sciences
4. Graduate Other area:__________________________________

9. How many years of work experience do you have?

1. None
2. 1 - 2 years
3. 3 – 5 years
4. 5 – 10 years
5. 10+ years

10. In regards to your proficiency in the use of a computer, do you consider yourself a:

1. Technical Guru
2. Expert
3. Intermediate
4. Novice
5. Beginner

11. Have you ever published a document on the World Wide Web

1. Yes
2. No

12. How many hours in a typical week do you use a computer?

1. None
2. 1 – 2 hours
3. 3 – 5 hours
4. 5 – 10 hours
5. 10 –15 hours
6. 15+ hours

13. What type of computer do you own?

1. PC Windows machine
2. Macintosh
3. Both
4. Other ________________
5. None

14. Is the computer you own a

1. Desktop
2. Laptop
3. Both
4. None

15. Do you have a computer at your residence?

Yes No

16. Do you have experience using a modem?

Yes No

17. Have you used (circle all that apply)

1. Systems editors
2. Html editors
3. Imaging software
4. Image scanners
5. ftp
6. telnet
7. encryption tools
8. Netscape
9. Microsoft Internet Explorer

18. Which computer applications do you primarily use:

1. Word processing
2. Spreadsheets
3. Presentation Software
4. Communications Software
5. Other

19. Have you ever created a command script?

1. Yes
2. No
3. Do not know

20. Have you ever created any type of these programs (check all that apply)

1. Basic
2. Pascal
3. C or C++
4. CGI
5. Cobal
6. Fortran
7. Java or J++
8. Other
9. None

Section 2: COMPUTER SECURITY KNOWLEDGE

21. Safeguarding a business entity information resources is essentially the overall responsibility of:

1. Chief Executive
2. Chief Information Officer
3. Secuity Officer
4. Outside Auditor
5. Systems Manager
6. Systems Administrator
7. Each User who uses the information resource

22. The terms: integrity, availability, control and audit ability have particular reference to

1. Computer security objectives
2. Systems performance criteria
3. Allocation of Audit Controls
4. Systems failures

23. With reference to systems security; risks and uncertainty mean the same

1. Agree
2. Disagree
3. Do Not Know

24. Creation of a written Systems Security Policy is: (check allthat apply)

1. Necessary
2. No necessary
3. Unnecessary
4. Intended to establish guidelines and responsibilities
5. Should be widely disseminated
6. Read once a year to all employees
7. Restricted to "need to know"

25. A security standard:

1. Provides criteria to assess requirements
2. Guideline for remedial action
3. Legal directive
4. Basis for legal action
5. Never used on trusted systems
6. First line defense

26. Logon Ids should be changed in accordance with

1. Systems administrators concepts
2. Security policy
3. Criteria based on systematic assessment of risks

27. Likelihood of threats means:

1. Threat and associated expectancy
2. Ratio of threat class and threat
3. Do not know

28. Systems security has no relationship with human resources policies:

1. Agree
2. Disagree
3. Do not know

29. Applications programming errors are not in the domain of Systems Security:

1. Yes
2. No
3. Do Not Know

30. Backup Planning is

1. Necessary
2. Typically the responsibility of the systems manager
3. Hazardous
4. Unnecessary

31. A vunerability in the domain of system security means:

1. A weakness that may be exploited
2. A glitch – not to worry
3. A patch that has not been applied

32. The terms vulnerability – exposure – risk means the same thing:

1. Agree
2. Disagree
3. Do not know

33. The EDP auditor brings the same technical skills to the systems audit, regardless whether the audit is external or internal

1. Agree
2. Disagree
3. Do not know

34. The conduct of "surprise" no notice types of a systems audit is a good way to evaluate the real level of security and actual operation of a system

1. Agree
2. Disagree
3. Dc not know

35. Systems auditing uses two major classes of programs

1. Debuggers
2. Data audit programs
3. Profilers
4. Source comparators
5. Firewalls
6. Do not know

36. Systems security can be conceptualized as a process oriented methodology to ensure that management si exercising adequate control and reasonable assurance over the reliable operation of critical computer systems necessary for the firm's operations

1. Agree
2. Disagree
3. Do not know

37. For applications design, check digits are typically used for:

1. Guard against transposition errors
2. Check for out of range errors
3. Secure against viruses

38. A computer virus is (check all that apply)

1. An applications program
2. Corrupts data
3. Interferes with the normal systems operations
4. Can copy itself
5. Can be transmitted by magnetic media
6. Can be hosted in network traffic

39. Production applications should be

1. Staged to tests hosts prior to production
2. Tested by some end users
3. Checked for controlled inputs and outputs

40. The primary purpose for encryption is

1. Protect sensitive data
2. Insuring none repudiation
3. Use of cipher codes
4. Do not know

41. Kerberos is an advanced type of

1. Authentication system
2. Applications programming assurance tool
3. Penetration tool
4. Hacker's society

42. A technical penetration technique involves working on weaknesses of the entire system

1. Yes
2. No
3. Do not know

43. There is an unfounded human tendency to believe that computer generated information is correct

1. Agree
2. Disagree
3. Do not know

44. A sniffer is a set of tools that can

1. Display network packets
2. Announce themselves
3. Assure data integrity
4. Do not know

45. A "Trojan Horse" is

1. A program that contains unauthorized functions
2. Can capture unintended data
3. Data verification tool
4. Do not know

46. A brute force attack is the exhaustive attempt to capture: (check all that apply)

1. Network data
2. Users Ids
3. Passwords
4. Do not know

47. Social engineering is one way to gain login and authentication data

1. Yes
2. No
3. Do not know

48. One Time Passwords are

1. Difficult to impersonate
2. Hard to implement
3. Require investments
4. Do not know

49. A Computer Emergency Response Team (CERT) is an organizational team that

1. Plans actions and responses to computer systems – accidents and intrusions
2. Guarantees protection and recovery events
3. Announces all vulnerabilities
4. Certifies people to have trusted access

50. Logic bombs typically reproduce themselves in other programs that are running on the system

1. Yes
2. No
3. Do Not Know

51. There are generally effective ways to prevent virus infections:

1. Agree
2. Disagree
3. Do not know

52. Typically "outsiders" consultants and contractors receive system security briefings

1. Agree
2. Disagree
3. Do not know

53. A router is a network host that receives messages and directs them to other nodes, hosts, or networks

1. Agree
2. Disagree
3. Do not know

54. A network typology is a pattern of link in a network, which typically include ring, bus, star or tree

1. Agree
2. Disagree
3. Do not know

55. Access controls are techniques for limiting access to resources based on riles and authentication information

1. Agree
2. Disagree
3. Do not know

56. A cookie is a password, set of data or keys that are transmitted to and from a client/server over a network

1. Agree
2. Disagree
3. Do not know

57. A firewall is a system of filters that mediate internal and external networks

1. Agree
2. Disagree
3. Do not know

58. The WWW is a cohesive view of the Internet, through which many protocols operate

1. Agree
2. Disagree
3. Do not know

59. Denial of service is deliberate action that prevents the system's normal functioning

1. Agree
2. Disagree
3. Do not know

60. A Grandfather cycle is a process for backup of data to insure that the proper data can be recovered

1. Agree
2. Disagree
3. Do not know

61. Social engineering is one way to gain login and authentication data

1. Agree
2. Disagree
3. Do not know

Section 3: SECURITY CONCERNS

62. Please rate your present concerns in the area of information/data security:

1. Network security ____________________
2. Integrating security systems ____________________
3. Monitoring user compliance with policies________________
4. Distributed computing security ____________________
5. Winning top management commitment__________________
6. Internet access ____________________
7. External/Remote access (dial in) ____________________

63. What do you perceive as obstacles in addressing security concerns within an organization (mark all that apply)

1. Lack of tools/security solutions
2. Lack of human resources]
3. Lack of management awareness of the importance of security
4. Lack of budget
5. Other

64. Please indicate the perceived level of threat of unauthorized information being disclosed due to the following:

1. Suppliers ______________________________
2. Competitors ______________________________
3. Employees who do not need to know______________________________
4. Customers ______________________________
5. Public interest groups ______________________________
6. Contracted service providers ______________________________
7. Computer "terrorists" ______________________________
8. Foreign governments ______________________________

Section 4: NETWORKS

65. Please rate the importance you assign to the following network issues:

1. Tampering or interference with intended operation of the network ______________________________
2. Loss of message integrity ______________________________
3. Loss of message confidentiality ______________________________
4. Inability to identify network users______________________________
5. Unavailability of network ______________________________
6. Unauthorized access via external remote dial in methods ______________________________

66. Should an organization actively monitor use of its local area and/or wide area networks?

1. Yes
2. No

67. Should an organization monitor network connections between yourself and trusted business partners?

1. Yes
2. No

Section 5: INTERNET AND ELECTRONIC COMMERCE

68. Are you satisfled with the overall level of security with your connection to the Internet?

1. Yes
2. No
3. No opinion

69. If your organization used electronic commerce for business transactions, what control techniques should be used?

Trading partner ID and profile verification
Functional acknowledgements
Application acknowledgements
Message authentication codes
Passwords
Control totals
Encryption
No control techniques needed

70. If you use electronic commerce what media do you use?

Internet
Leased line
Magnetic media
Intranet
Dialup
Other
(specify):____

71. What control techniques related to the Internet should an organization use?

Encryption
Passwords
One time (token based) passwords
Firewalls (application based, workstation based, and/or router based)

Section 5: BUSINESS CONTINUITY PLAN

72. Is a business continuity plan important within an organization

1. Yes
2. No
3. Do not know

73. Which of the following should be in a business continuity planning within an organization? (Mark all that you feel should apply)

1. No formal business continuity plan
2. End user computing
3. Recovery of mission critical business processes
4. Complete restoration
5. Enterprise network (voice and data)
6. LANs
7. Operations center

Section 7: SECURITY POLICY

74. Which of the following should be included in a company's formal corporate information/data security policy?

Centralized security administration
Data classification
Records management
Electronic commerce services
External access
End user computing
Personnel security non disclosure agreements
Surveillance and monitoring
Incident response and reporting
Business continuity planning corporate wide
None of the above / no formal policy

75. Does an organization need a stand alone information security orientation program for new employees?

1. Yes
2. No

76. Should an organization implement security measures on all of their systems and information?

1. Yes
2. No

77. If no, what information should be exempt from security measures?

78. Where does an organization's most dangerous security threat come from

1.From outside the organization
2.From inside the organization

79. What are the key security issues that concern you?

No issues concern me

Information Security
Internet Security
Intranet Security
Virus Infection
Access Control
Firewalls
Communications Security
Biometrics
Computer Forensics
Others
Business Security
E commerce
Remote Access
Software Licensing
Security Administration
Disaster Recovery/Continuity
Year 2000
Training
Industrial Espionage

80. How frequently do you want/need information on your key security concerns

1. Monthly
2. Bimonthly
3. Quarterly

4. Annually
5. Never

81. Do you feel it is important for senior management to be involved in information and data security?

Whom do you believe that the senior information security person of an organization should report to? ______________________________
Head of information systems ______________________________
Department head within IS ______________________________
Non-IS executive ______________________________
Internal audit ______________________________
Other ______________________________

APPENDIX B: RESEARCH PARTICPANT AGREEMENT

PARTICIPANT AGREMENT

Project Title: Information Security Survey

Purpose:
The purpose of this research is to gather information about attitudes and knowledge of graduate students of the University of Texas at Austin Graduate School of Business.

Importance:
While you do not have to participate in this research effort, your response will help others more effectively learn about information security.

Participation:
Your participation in this study is voluntary. Any participant may refuse to participate or may withdraw at any time without creating any harmful consequences whatsoever. The participant understands that the researcher may drop the participant from the study at any time.

Contact:
Information about this study was discussed with me by Cherie Long. I can reach her at any time I have questions by calling (512) 338-4914.

Acknowledgement:
The researcher asks that you carefully read and sign the following agreement, if you agree to participate.

Date:______________________________
Signed:____
Printed Name:____
Address: ____
City: ____________________________ State: _______________
Zip:__________
Home Phone: ___________________ Work Phone:_____________

APPENDIX C: AGARWAL, TANNIRU & WILEMON INNOVATION MODEL

Definitions of Implementation Strategies (Agarwal, Tanniru, & Wilemon, 1995).

Support - The organization makes resources available to potential adopter to use, but permits individuals to voluntarily use the innovation in an exploratory manner. This is a passive strategy, since the goal is to allow the innovation to prove itself first, through informal experimentation and usage, and then to allow the innovation to spread, through positive word-of-mouth recommendations. Specific actions must be taken by the organization, which includes acquiring the innovation, defining product standards, developing the necessary hardware and software infrastructure, providing training, and ensuring the availability of technical support.

Advocacy - A strategy in which the organization takes a proactive role, compared to support. In this strategy, the organization actively ensures that the innovation becomes adopted among a subset of the potential adopter base -- for example, using a small number of pilot projects. Management must guarantee that the innovation becomes adopted in one or a few work groups, and offers training and other support activities. In addition, it ensures that necessary changes are implemented in job roles, coordination processes among adopters, departmental structure, etc, that are required to exploit the innovation. Management takes an active role in diffusing the innovation to the initial adopters, by using persuasive communication and possibility, mandating usage.

Total Commitment - This strategy is described as the simultaneous combination of the support and advocacy strategies. In this case, however, the innovation is adopted across the entire target adopter population, rather than in a small number of pilot groups. This strategy works best when "the organization is useful, and is totally committed to do what is necessary" to ensure that it is adopted.

APPENDIX D: SURVEY RESULT TABLES

Table 1

Graduate Program

Category	n	%	Cum %
MBA	8	33%	33%
PH.D	1	4%	37%
MPA	15	63%	100%

Table 2

Major Concentration Area of Degree

	n	%	Cum %
IM	18	35%	35%
Accounting	14	27%	62%
Audit	10	20%	82%
Other	6	12%	95%
Finance	1	2%	97%
Marketing	1	2%	99%
Management	1	2%	100%

Table 3

Work Experience

	n	%	Cum %
None	20	39%	39%
1 – 2 years	7	13%	52%
3 –5 years	11	21%	74%
5 – 10 years	5	10%	84%
10+ years	8	16%	100%

Table 4

Reason for Taking Course

	n	%	Cum %
gen interest	31	59.62%	59.62%
rec advisor	8	15.38%	75.00%
course req	7	13.46%	88.46%
rec employer	6	11.54%	100.00%
no reason	0	0.00%	100.00%

Table 5

Information Audit Professional

	n	**%**	**Cum %**
Yes	25	49.02%	49.02%
No	16	31.37%	80.39%
Do not know	10	19.61%	100.00%

Table 6

Prior Systems or Audit Training

	n	**%**	**Cum %**
Extensive	0	0.%	0%
Some	18	35%	35%
None	34	65%	100%

Table 7

Undergraduate Education

	n	**%**	**Cum %**
Liberal Arts	12	23%	23%
Business	27	52%	75%
Engineering/Sciences	13	25%	100%

Table 8

Computer Proficiency

	n	%	Cum %
Technical Guru	2	3.85%	3.85%
Expert	11	21.15%	25.00%
Intermediate	27	51.92%	76.92%
Novice	12	23.08%	100.00%

Table 9

Hours Per Week Work on Computer

	n	%	Cum %
None			
1 –2 hours			
3 – 5 hours	1	1.92%	1.92%
5 –10 hours	10	19.23%	21.15%
10 – 15 hours	12	23.08%	44.23%
15+ hours	20	38.46%	82.69%

Table 10

Type of Computer System Used

	n	%	Cum %
PC Windows	47	90.38%	90.38%
Macintosh	1	1.92%	92.31%
Both	2	3.85%	96.15%
Other	1	1.92%	98.08%
None	1	1.92%	100.00%

Table 11

Do you have a computer at home

	n	%	Cum %
Yes	49	94.%	94.%
No	3	6%	100%

Table 12

Type of Computer Owned

	n	%	Cum %
Desktop	33	64.71%	64.71%
Laptop	5	9.80%	74.51%
Both	13	25.49%	100.00%

Table 13

Experience using modem

	n	%	Cum %
Yes	50	96.15%	96.15%
No	2	3.85%	100.00%

Table 14

Published on World Wide Web

	n	%	Cum %
Yes	30	58.82%	58.82%
No	21	41.18%	100.00%

Table 15

Use of Internet Tools

Tool	n	%
Netscape Browser	46	88.46%
Internet Explorer Browser	38	73.08%
File Transfer Protocol (FTP)	33	63.46%
Telnet	33	63.46%
Scanners	27	51.92%
Html editors	25	48.08%
Imaging software	19	36.54%
Systems editors	10	19.23%
Encryption tools	10	19.23%

Table 16

Computer Applications Used

	n	%
Word Processors	50	96.15%
Spreadsheets	43	82.69%
Presentation Software	28	53.85%
Communications	33	63.46%
Other	11	21.15%

Table 17

Written a Command Script

	n	%	Cum %
Yes	17	33.33%	33.33%
No	17	33.33%	66.67%
Do Not Know	17	33.33%	100.00%

Table 18

Prior Programming Experience

Language	n	%
Basic	33	63.46%
Pascal	20	38.46%
C or C++	14	26.92%
Other	12	23.08%
None	10	19.23%
Cobol	9	17.31%
Fortran	9	17.31%
Java	7	13.46%
CGI	6	11.54%

Table 19

ANOVA Analysis for Security Knowledge

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Prior Systems or Audit Training	Between Groups	3.069	19	.162	.594	.883
	Within Groups	8.700	32	.272		
	Total	11.769	51			
Computer Proficiency	Between Groups	12.127	19	.638	1.092	.402
	Within Groups	18.700	32	.584		
	Total	30.827	51			
Graduate Program	Between Groups	18.667	19	.982	1.003	.483
	Within Groups	31.333	32	.979		
	Total	50.000	51			
Information/Audit Professional	Between Groups	12.088	19	.636	1.066	.426
	Within Groups	18.500	31	.597		
	Total	30.588	50			
Major Concentration	Between Groups	84.690	19	4.457	1.150	.355
	Within Groups	120.133	31	3.875		
	Total	204.824	50			
Undergraduate Education	Between Groups	9.097	19	.479	.965	.521
	Within Groups	15.883	32	.496		
	Total	24.981	51			
Work Experience	Between Groups	50.578	19	2.662	1.372	.212
	Within Groups	60.167	31	1.941		
	Total	110.745	50			

Table 20

Crosstabulations of
Preceived Obstacles in Addressing Security Concerns to IV
Computer Proficiency

```
                    Count  I
                   Row pct I                                          Row
                           I                                         Total
                           I Expert  I Inter   I Novice  I
                           +---------+---------+---------+
                           I      3  I     11  I      2  I     16
lack of budget             I   18.8  I   68.8  I   12.5  I   20.8
                           +---------+---------+---------+
                           I      5  I     11  I      1  I     17
lack of human resour       I   29.4  I   64.7  I    5.9  I   22.1
                           +---------+---------+---------+
                           I      5  I     16  I      3  I     24
lack of management a       I   20.8  I   66.7  I   12.5  I   31.2
                           +---------+---------+---------+
                           I      0  I      2  I      0  I      2
Obstacles other            I     .0  I  100.0  I     .0  I    2.6
                           +---------+---------+---------+
                           I      5  I     12  I      1  I     18
lack of tools/securi       I   27.8  I   66.7  I    5.6  I   23.4
                           +---------+---------+---------+
                   Column       18        52         7         77
                    Total     23.4      67.5       9.1
```

Table 21

Crosstabulations of Perceived Obstacles in Addressing Security Concerns to IV Information Professional

	Yes	No	Don't Know
lack of budget	7 43.8	4 25.0	5 31.3
lack of human resour	8 47.1	5 29.4	4 23.5
lack of management a	11 45.8	6 25.0	7 29.2
Obstacles other	0 .0	0 .0	2 100.0
lack of tools/securi	9 50.0	4 22.2	5 27.8
Column Total	35 45.5	19 24.7	23 29.9

Table 22

Crosstabulations of Perceived Obstacles in Addressing Security Concerns to IV Major Concentration

	IM	Audit	Acct	Mgt
lack of budget	7 43.8	4 25.0	3 18.8	0 .0
lack of human resour	8 47.1	3 17.6	4 23.5	0 .0
lack of management a	11 45.8	5 20.8	5 20.8	1 4.2
Obstacles other	1 50.0	0 .0	1 50.0	0 .0
lack of tools/securi	6 33.3	5 27.8	3 16.7	1 5.6

Table 23

Crosstabulations of Preceived Obstacles in Addressing Security Concerns to IV Prior Security Systems or Audit Training

```
              Row pct I                   Row
                      I                  Total
                      I   Some I   None I
                      +--------+--------+--------+
                      I      4 I     12 I    16
lack of budget        I  25.0  I  75.0  I  20.8
                      +--------+--------+
                      I      7 I     10 I    17
lack of human resour  I  41.2  I  58.8  I  22.1
                      +--------+--------+
                      I      9 I     15 I    24
lack of management a  I  37.5  I  62.5  I  31.2
                      +--------+--------+
                      I      0 I      2 I     2
Obstacles other       I    .0  I 100.0  I   2.6
                      +--------+--------+
                      I      6 I     12 I    18
lack of tools/securi  I  33.3  I  66.7  I  23.4
                      +--------+--------+
               Column       26       51       7
```

Table 24

Crosstabulations of
Preceived Obstacles in Addressing Security Concerns to IV
Graduate Program

```
                 Count     I MBA      Ph.D      MPA       PPA
                           +--------+--------+--------+--------+
                           I     3  I     1  I    11  I     1  I
  lack of budget           I  18.8  I   6.3  I  68.8  I   6.3  I
                           +--------+--------+--------+--------+
                           I     3  I     1  I    10  I     3  I
  lack of human resoures   I  17.6  I   5.9  I  58.8  I  17.6  I
                           +--------+--------+--------+--------+
                           I     5  I     1  I    15  I     3  I
  lack of management a     I  20.8  I   4.2  I  62.5  I  12.5  I
  awareness of importance
  of security              +--------+--------+--------+--------+
                           I     0  I     0  I     2  I     0  I
  Obstacles other          I    .0  I    .0  I 100.0  I    .0  I
                           +--------+--------+--------+--------+
                           I     3  I     1  I    12  I     2  I
  lack of tools/security   I  16.7  I   5.6  I  66.7  I  11.1  I
+--------+--------+--------+--------+
                Column        14         4        50         9
                 Total      18.2       5.2      64.9      11.7
```

Table 25

Crosstabulations of
Preceived Obstacles in Addressing Security Concerns to IV
Undergraduate Education

```
                    I LiberalIBusinessI Eng/SciI
                    +--------+--------+--------+
                    I     3  I     9  I     4  I
lack of budget      I  18.8  I  56.3  I  25.0  I
                    +--------+--------+--------+
                    I     3  I     9  I     5  I
lack of human resoures I  17.6  I  52.9  I  29.4  I
                    +--------+--------+--------+
                    I     4  I    14  I     6  I
lack of management a I  16.7  I  58.3  I  25.0  I
                    +--------+--------+--------+
                    I     0  I     1  I     1  I
Obstacles other     I    .0  I  50.0  I  50.0  I
                    +--------+--------+--------+
                    I     3  I     9  I     6  I
lack of tools/securi I  16.7  I  50.0  I  33.3  I
                    +--------+--------+--------+
            Column       13       42       22
             Total     16.9     54.5     28.6
```

Table 26

Crosstabulations of Perceived Obstacles in Addressing Security Concerns to IV Work Experience

```
                Count  I None     I 1 - 2  I 3 - 5  I 5 - 10 I
               Row pct I          I years  I years  I years   I
               --------+----------+--------+--------+--------+-
                       I      6   I     2  I     3  I      1  I
  lack of budget       I   37.5   I  12.5  I  18.8  I    6.3  I
                       +----------+--------+--------+--------+
                       I      5   I     4  I     2  I      1  I
  lack of human resoures I 29.4   I  23.5  I  11.8  I    5.9  I
                       +----------+--------+--------+--------+
                       I     10   I     4  I     3  I      1  I
  lack of management a I   41.7   I  16.7  I  12.5  I    4.2  I
                       +----------+--------+--------+--------+
                       I      1   I     1  I     0  I      0  I
  Obstacles other      I   50.0   I  50.0  I    .0  I     .0  I
                       +----------+--------+--------+--------+
                       I      7   I     3  I     1  I      1  I
  lack of tools/security I 38.9   I  16.7  I   5.6  I    5.6  I
                       +--------+--------+--------+--------+--
Column        29        14         9         4        21
                Total     37.7      18.2      11.7      5.2
```

Table 27

Crosstabulations of
Present Concerns in Area of Information/Data Security to IV Computer Proficiency

```
                 Count  I
               Row pct  I                                  Row
                        I                                  Total
                        I Expert  I Inter   I Novice  I
               ---------+---------+---------+---------+
                     1  I      0  I      4  I      0  I       4
Not Important           I     .0  I  100.0  I     .0  I     1.8
                        +---------+---------+---------+
                     2  I      5  I     28  I      0  I      33
Somewhat Important      I   15.2  I   84.8  I     .0  I    14.9
                        +---------+---------+---------+
                     3  I     23  I     43  I     13  I      79
Important               I   29.1  I   54.4  I   16.5  I    35.6
                        +---------+---------+---------+
                     4  I     25  I     69  I     12  I     106
Extremely Important     I   23.6  I   65.1  I   11.3  I    47.7
                        +---------+---------+---------+
                Column        53       144        25        222
                 Total      23.9      64.9      11.3      100.0
```

Table 28

Crosstabulations of Present Concerns in Area of Information/Data Security to IV Information Professional

Count Row pct	Yes	No	Don't Know	Row Total
Not Important	3 75.0	0 .0	1 25.0	4 1.8
Somewhat Important	14 42.4	10 30.3	9 27.3	33 14.9
Important	50 63.3	17 21.5	12 15.2	79 35.6
Extremely Important	40 37.7	25 23.6	41 38.7	106 47.7
Column Total	107 48.2	52 23.4	63 28.4	222 100.0

Table 29

Crosstabulations of Present Concerns in Area of Information/Data Security to IV Major Concentration

	IM	Audit	Acct	Mgt
Not Important	4 100.0	0 .0	0 .0	0 .0
Somewhat Important	13 39.4	10 30.3	5 15.2	2 6.1
Important	35 44.3	25 31.6	10 12.7	0 .0
Extremely Important	47 44.3	10 9.4	28 26.4	7 6.6
Column Total	99 44.6	45 20.3	43 19.4	9 4.1

Table 30

Crosstabulations of Present Concerns in Area of Information/Data Security to IV Prior Systems or Audit Training

Count Row pct		Yes	No	Row Total
Not Important	1	0 .0	4 100.0	4 1.8
Somewhat Important	2	13 39.4	20 60.6	33 14.9
Important	3	42 53.2	37 46.8	79 35.6
Extremely Important	4	34 32.1	72 67.9	106 47.7
Column Total		89 40.1	133 59.9	222 100.0

Table 31

Crosstabulations of Present Concerns in Area of Information/Data Security to IV Graduate Program

	MBA	Ph.D	MPA	PPA
Not Important	0 .0	2 50.0	2 50.0	0 .0
Somewhat Important	6 18.2	4 12.1	20 60.6	3 9.1
Important	13 16.5	1 1.3	57 72.2	8 10.1
Extremely Important	26 24.5	2 1.9	64 60.4	14 13.2
Column Total	45 20.3	9 4.1	143 64.4	25 11.3

Table 32

Crosstabulations of
Present Concerns in Area of Information/Data Security to IV Undergraduate Education

```
                  Count  ILiberal  Business Engineer
                Row pct  IArts              /Sciences  Row
                         +--------+--------+--------+
                      1  I      0 I      2 I      2 I     4
Not Important            I     .0 I   50.0 I   50.0 I   1.8
                         +--------+--------+--------+
                      2  I      3 I     20 I     10 I    33
Somewhat Important       I    9.1 I   60.6 I   30.3 I  14.9
                         +--------+--------+--------+
                      3  I      8 I     54 I     17 I    79
Important                I   10.1 I   68.4 I   21.5 I  35.6
                         +--------+--------+--------+
                      4  I     22 I     50 I     34 I   106
Extremely Important      I   20.8 I   47.2 I   32.1 I  47.7
                         +--------+--------+--------+
                 Column        33      126       63     222
                  Total      14.9     56.8     28.4   100.0
```

Table 33

Crosstabulations of
Present Concerns in Area of Information/Data Security to IV Work Experience

```
                    Count  INone      1 - 2     3 - 5     5 - 10    10+
                  Row pct  I          years     years     years     years
                           I       1  I     2  I     3  I     4  I     5  I
                   --------+----------+--------+--------+---------+---------+
                        1  I       0  I     2  I     0  I     0  I     2  I
  Not Important            I      .0  I  50.0  I    .0  I    .0  I  50.0  I
                           +----------+--------+--------+---------+---------+
                        2  I      16  I     8  I     0  I     1  I     8  I
  Somewhat Important       I    48.5  I  24.2  I    .0  I   3.0  I  24.2  I
                           +----------+--------+--------+---------+---------+
                        3  I      42  I    18  I    10  I     4  I     5  I
  Important                I    53.2  I  22.8  I  12.7  I   5.1  I   6.3  I
                           +----------+--------+--------+---------+---------+
                        4  I      32  I    17  I    17  I     4  I    36  I
  Extremely Important      I    30.2  I  16.0  I  16.0  I   3.8  I  34.0  I
                           +----------+--------+--------+---------+---------+
                   Column         90        45       27         9        51
                    Total       40.5      20.3     12.2       4.1      23.0
```

Table 34

Frequency Distribution of
Present Concerns in the Area of Information/Data Security

	Not imp	Somewhat	Imp	Extremely
network security		4%	16%	80%
multiple logons and passwords		36%	40%	24%
integrating security systems	4%	8%	41%	45%
end uer computing security		8%	36%	56%
monitoring user compliance	4%	20%	45%	29%
distributed computing security		13%	56%	30%
winning top management	4%	16%	12%	72%
internet access	4%	16%	36%	44%
external/remote access	4%	12%	36%	48%

Table 35

Frequency Distribution of
Obstacles in Addressing Security Concerns within an Organization

	n	%
lack of tools/security solutions	19	36.54%
lack of human resources	18	34.62%
lack of management awareness	25	48.08%
lack of budget	17	32.69%
other	2	3.85%

Table 36

Frequency Distribution of
Preceived Level of Threat of Unauthorized Information Being Disclosed Due to:

	Not a Threat	Potential Threat	Threat	Serious Threat
	%	%	%	%
Suppliers		54%	33%	12.5%
Competitors		12%	40%	48%
Emp who do not need to know	4%	36%	44%	16%
Customers	4%	52%	32%	12%
Public Interest Groups	4%	36%	28%	32%
Contracted Service Providers		28%	52%	20%
Computer Terrorists		4%	28%	68%
Foreign Governments	4%	12%	32%	52%

Table 37

Frequency Distribution of
Importance Assigned to Network Issues

	Not	Somewhat		Extremely
	Important	Important	Important	Important
	%	%	%	%
tampering or interference	12%	12%	24%	76%
loss messge integrity		12%	16%	72%
loss message confidentiality		4%	24%	72%
inability to identify network users		12%	32%	56%
unavailability of network		4%	12%	84%
unauthorized access via remote		4%	20%	76%

Table 38

Frequency Distribution
Should an Organization Monitor Use of Local Area and/or Wide Area Networks

	n	%	Cum %
Yes	23	92%	92%
No	2	8%	100%

Table 39

Frequency Distribution of
Shouid an Organization Monitor Network Connections Between Yourself and Trusted Business Partners

	n	&	Cum %
Yes	22	88%	88%
No	3	12%	100%

Table 40

Crosstabulations of
Importance Assigned to Network Issue by IV Computer Proficiency

```
                     Count   I Expert  Intermed Novice
                     --------+--------+--------+--------+
                             I     2  I     7  I     0  I     9
Somewhat Important           I        I        I        I  36.0
                             +--------+--------+--------+
                             I     5  I    24  I     3  I    32
Important                    I        I        I        I 128.0
                             +--------+--------+--------+
                             I    29  I    65  I    15  I   109
Extremely Important          I        I        I        I 436.0
                             +--------+--------+--------+
                    Column         6       16        3       25
                     Total      24.0     64.0     12.0    100.0
```

Table 41

Crosstabulations of
Importance Assigned to Network Issue by IV Information Professional

```
                     Info Prof  Not IP   Do Not Know
           ---------+---------+---------+---------+
                  2  I      3  I      3  I      3  I      9
Somewhat Important   I         I         I         I   36.0
                     +---------+---------+---------+
                  3  I     18  I      8  I      6  I     32
Important            I         I         I         I  128.0
                     +---------+---------+---------+
                  4  I     51  I     25  I     33  I    109
Extremely Important  I         I         I         I  436.0
                     +---------+---------+---------+
             Column        12         6         7        25
              Total      48.0      24.0      28.0     100.0
```

Table 42

Crosstabulations of
Importance Assigned to Network Issue by IV Major Concentration

```
              Count  I   IM    I Audit   I  Acct   I Mgt     I Other
           ---------+---------+---------+---------+---------+---------+
                     I      4  I      3  I      1  I      0  I      1  I
Somewhat Important   I         I         I         I         I         I
                     +---------+---------+---------+---------+---------+
                     I     13  I     11  I      4  I      0  I      4  I
Important            I         I         I         I         I         I
                     +---------+---------+---------+---------+---------+
                     I     49  I     16  I     25  I      6  I     13  I
Extremely Important  I         I         I         I         I         I
                     +---------+---------+---------+---------+---------+
             Column        11         5         5         1         3
              Total      44.0      20.0      20.0       4.0      12.0
```

Table 43

Crosstabulations of
Importance Assigned to Network Issue by IV Prior Systems or Audit Training

```
                     Count   I Some      None
                   --------+---------+---------+
                           I       6 I       3 I       9
Somewhat Important         I         I         I    36.0
                           +---------+---------+
                           I      13 I      19 I      32
Important                  I         I         I   128.0
                           +---------+---------+
                           I      41 I      68 I     109
Extremely Important        I         I         I   436.0
                           +---------+---------+
                    Column        10        15        25
                     Total      40.0      60.0     100.0
```

Table 44

Crosstabulations of
Importance Assigned to Network Issue by IV Graduate Program

```
                           I IM      I  Audit I  Acct   I    Mkt I
                   --------+---------+---------+---------+---------+
                         2 I       0 I       1 I       7 I       1 I       9
Somewhat Important         I         I         I         I         I    36.0
                           +---------+---------+---------+---------+
                         3 I       4 I       2 I      23 I       3 I      32
Important                  I         I         I         I         I   128.0
                           +---------+---------+---------+---------+
                         4 I      26 I       3 I      66 I      14 I     109
Extremely Important        I         I         I         I         I   436.0
                           +---------+---------+---------+---------+
                    Column         5         1        16         3        25
                     Total      20.0       4.0      64.0      12.0     100.0
```

Table 45

Crosstabulations of Importance Assigned to Network Issue by IV Work Experience

```
                       I None   I 1-2 yrsI 3-5 yrsI5-10 yrsI 10+ yrsI
$ISSUES        --------+--------+--------+--------+--------+--------+
                     2 I     4  I     4  I     0  I     0  I     1  I
  Somewhat Important   I        I        I        I        I        I
                       +--------+--------+--------+--------+--------+
                     3 I    14  I     8  I     6  I     1  I     3  I
  Important            I        I        I        I        I        I
                       +--------+--------+--------+--------+--------+
                     4 I    42  I    18  I    12  I     5  I    32  I
  Extremely Important  I        I        I        I        I        I
                       +--------+--------+--------+--------+--------+
               Column      10        5        3        1        6
```

Table 46

Crosstabulations of Importance Assigned to Network Issue by IV Undergraduate Education

```
                Count  ILiberal  Business Engineering/
                       IArts              Sciences   Row
                       I     1  I     2  I     3  I
$ISSUES        --------+--------+--------+--------+
                     2 I     0  I     7  I     2  I     9
  Somewhat Important   I        I        I        I  36.0
                       +--------+--------+--------+
                     3 I     3  I    22  I     7  I    32
  Important            I        I        I        I 128.0
                       +--------+--------+--------+
                     4 I    21  I    55  I    33  I   109
  Extremely Important  I        I        I        I 436.0
                       +--------+--------+--------+
               Column       4        14        7        25
                Total     16.0     56.0     28.0    100.0
```

Table 47

Frequency Distribution
Satisfaction with Overall Level of Security of Connection to Internet

Responses	25	%	Cum %
Yes	5	20%	20%
No	12	48%	68%
No Opinion	8	32%	100%

Table 48

Frequency Distribution
Control Techniques Used for Electronic Commerce

Response	N	%
Message authentication codes	22	88%
Trading partner ID and profile verification	18	72%
Passwords	17	68%
Encryption	17	68%
Functional acknowledgements	13	52%
Application acknowledgements	12	48%
Control totals	12	48%
No control techniques needed	1	4%

Table 49

Frequency Distribution
Media Used for Electronic Commerce

Media	n	%
Internet	20	80%
Dialup	7	28%
Leased line	5	20%
Intranet	2	8%
Magnetic media	1	4%
Other (specify	0	0

Table 50

Frequency Distribution
Control Techniques Related to Internet

Passwords	20	80%
Firewalls	19	76%
Encryption	18	72%
One time (token based) passwords	7	28%

Table 51

Crosstabulations of
Internet Controls to IV Computer Expertise

```
                  Encryption Password  1x Pwd  Firewalls
          --------+--------+--------+--------+--------+
                2 I      6 I      4 I      1 I     12
Expert            I   50.0 I   33.3 I    8.3 I   25.0
                  +--------+--------+--------+--------+
                3 I     10 I     13 I      4 I     30
Intermediate      I   33.3 I   43.3 I   13.3 I   62.5
                  +--------+--------+--------+--------+
                4 I      2 I      2 I      1 I      6
Novice            I   33.3 I   33.3 I   16.7 I   12.5
                  +--------+--------+--------+--------+
           Column       18       19        5        6
            Total     37.5     39.6     12.5    100.0
```

Table 52

**Crosstabulations of
Electronic Commerce Controls to IV Computer Proficiency**

```
                         Count  IApplicat  Control   Encrypt   Function  Message
                       Row pct  I          Totals              Ack       Authenti
                       --------+---------+---------+---------+---------+---------+
                                I     0   I     2   I     5   I     2   I     6   I
  Expert                        I    .0   I   8.7   I  21.7   I   8.7   I  26.1   I
                                +---------+---------+---------+---------+---------+
                                I    10   I     8   I    10   I     9   I    14   I
  Intermediate                  I  13.5   I  10.8   I  13.5   I  12.2   I  18.9   I
                                +---------+---------+---------+---------+---------+
                                I     1   I     1   I     1   I     1   I     1   I
  Novice                        I  14.3   I  14.3   I  14.3   I  14.3   I  14.3   I
                                +---------+---------+---------+---------+---------+
                        Column      11        11        16        12        21
                         Total    10.6      10.6      15.4      11.5      20.2
```

Table 52 continued

**Crosstabulations of
Electronic Commerce Controls to IV Computer Proficiency**

```
                         Count  IPassword Trading   Partner
  INDEPENDENT VARIABLE:         +---------+---------+---------+
                             2  I     4   I     4   I    23
  Expert                        I  17.4   I  17.4   I  22.1
                                +---------+---------+
                             3  I    11   I    12   I    74
  Intermediate                  I  14.9   I  16.2   I  71.2
                                +---------+---------+
                             4  I     1   I     1   I     7
  Novice                        I  14.3   I  14.3   I   6.7
                                +---------+---------+
                        Column      16        17       104
                         Total    15.4      16.3     100.0
```

Table 53

Crosstabulations
Electronic Commerce Controls to Information Professional

```
                 Count  IApplicat Control  Encrypt  Function Message
               Row pct  I         Totals            Ack      Authent
INDEPENDENT VARIABLE:   +--------+--------+--------+--------+
                     1  I     10 I     11 I      2 I      3 I     26
                        I   38.5 I   42.3 I    7.7 I   11.5 I   54.2
                        +--------+--------+--------+--------+
                     2  I      4 I      3 I      3 I      2 I     12
                        I   33.3 I   25.0 I   25.0 I   16.7 I   25.0
                        +--------+--------+--------+--------+
                     3  I      4 I      5 I      0 I      1 I     10
                        I   40.0 I   50.0 I     .0 I   10.0 I   20.8
                        +--------+--------+--------+--------+
                Column        18       19        5        6       48
                 Total      37.5     39.6     10.4     12.5    100.0
```

Table 53 continued

Crosstabulations
Electronic Commerce Controls to Information Professional

```
 Count  I Appl     Control  Encrypt  Function Message
        +--------+--------+--------+--------+--------+
     1  I      4 I      4 I      8 I      5 I     11 I
        I    8.3 I    8.3 I   16.7 I   10.4 I   22.9 I
        +--------+--------+--------+--------+--------+
     2  I      2 I      2 I      3 I      3 I      5 I
        I   10.0 I   10.0 I   15.0 I   15.0 I   25.0 I
        +--------+--------+--------+--------+--------+
     3  I      5 I      5 I      5 I      4 I      5 I
        I   13.9 I   13.9 I   13.9 I   11.1 I   13.9 I
        +--------+--------+--------+--------+--------+
Column        11       11       16       12       21
 Total      10.6     10.6     15.4     11.5     20.2
```

Table 53 continued

Crosstabulations
Electronic Commerce Controls to Information Professional

```
                    Count  IPassword Trading
                  Row pct  I         Partner    Row
INDEPENDENT VARIABLE --------+--------+--------+
        IM Professional    I      8  I      8  I    48
                           I   16.7  I   16.7  I  46.2
                           +--------+--------+
Not an IM Professional     I      2  I      3  I    20
                           I   10.0  I   15.0  I  19.2
                           +--------+--------+
            Do Not Know    I      6  I      6  I    36
                           I   16.7  I   16.7  I  34.6
                           +--------+--------+
                 Column        16       17       104
                  Total       15.4     16.3     100
```

Table 54

Crosstabulations of
Electronic Commerce Controls to IV Major Concentration

```
                   Count  IApplicat Control  Encrypt  Function Message
                 Row pct  I         Totals            Ack      Authenti
INDEPENDENT VARIABLE:     --------+--------+--------+--------+--------+
                     IM   I     9  I     9  I     2  I     2  I    22
                          I  40.9  I  40.9  I   9.1  I   9.1  I  45.8
                          +--------+--------+--------+--------+
                  Audit   I     2  I     4  I     1  I     0  I     7
                          I  28.6  I  57.1  I  14.3  I    .0  I  14.6
                          +--------+--------+--------+--------+
                   Acct   I     3  I     3  I     1  I     2  I     9
                          I  33.3  I  33.3  I  11.1  I  22.2  I  18.8
                          +--------+--------+--------+--------+
                    Mgt   I     1  I     1  I     0  I     1  I     3
                          I  33.3  I  33.3  I    .0  I  33.3  I   6.3
                          +--------+--------+--------+--------+
                  Other   I     3  I     2  I     1  I     1  I     7
                          I  42.9  I  28.6  I  14.3  I  14.3  I  14.6
                          +--------+--------+--------+--------+
                 Column        18       19        5        6      48
                  Total       37.5     39.6     10.4     12.5   100.0
```

Table 54 continued

Crosstabulations of
Electronic Commerce Controls to IV Major Concentration

```
                        Count  IApplicat Control  Encrypt  Function Message
                      Row pct  IAcknowl  Totals            Acknow   Auth
INDEPENDENT VARIABLE: --------+--------+--------+--------+--------+----
                            1  I     7  I     5  I     6  I     6  I     8  I
                               I  14.6  I  10.4  I  12.5  I  12.5  I  16.7  I
                               +--------+--------+--------+--------+--------+
                            2  I     0  I     1  I     2  I     0  I     5  I
                               I    .0  I   8.3  I  16.7  I    .0  I  41.7  I
                               +--------+--------+--------+--------+--------+
                            4  I     3  I     3  I     4  I     4  I     4  I
                               I  12.5  I  12.5  I  16.7  I  16.7  I  16.7  I
                               +--------+--------+--------+--------+--------+
                            6  I     1  I     1  I     1  I     1  I     1  I
                               I  14.3  I  14.3  I  14.3  I  14.3  I  14.3  I
                               +--------+--------+--------+--------+--------+
                            7  I     0  I     1  I     3  I     1  I     3  I
                               I    .0  I   7.7  I  23.1  I   7.7  I  23.1  I
                               +--------+--------+--------+--------+--------+
                       Column        11       11       16       12       21
                        Total      10.6     10.6     15.4     11.5     20.2
```

Table 54 continued

Crosstabulations
Electronic Commerce Controls to Major Concentration

```
                   Count  IPassword Trading Partners
INDEPENDENT VARIABLE:     +--------+--------+
                     IM   I      7 I      9 I    48
                          I   14.6 I   18.8 I  46.2
                          +--------+--------+
                  Audit   I      2 I      2 I    12
                          I   16.7 I   16.7 I  11.5
                          +--------+--------+
                   Acct   I      3 I      3 I    24
                          I   12.5 I   12.5 I  23.1
                          +--------+--------+
                    Mgt   I      1 I      1 I     7
                          I   14.3 I   14.3 I   6.7
                          +--------+--------+
                  Other   I      3 I      2 I    13
                          I   23.1 I   15.4 I  12.5
                          +--------+--------+
                 Column         16       17     104
                  Total       15.4     16.3  100.00
```

Table 55

Crosstabulations
Internet Controls to Prior Systems or Audit Training

```
 Count   IFirewall Password Satisfac 1x Token

--------+--------+--------+--------+--------+
       2 I      8 I      6 I      4 I      3 I     21
         I   38.1 I   28.6 I   19.0 I   14.3 I   43.8
         +--------+--------+--------+--------+
       3 I     10 I     13 I      1 I      3 I     27
         I   37.0 I   48.1 I    3.7 I   11.1 I   56.3
         +--------+--------+--------+--------+
Column         18       19        5        6       48
 Total       37.5     39.6     10.4     12.5    100.0
```

Table 56

*** CROSSTABULATION ***
INDEPENDENT VARIABLE: Prior Systems or Audit Training by $ECCTR (tabulating 1) E commerce Controls

```
                  Count  IApplicat Control  Encrypti Function Message
                Row pct  Iack      Totals            Ackno    Authenti
INDEPENDENT VARIABLE:    +--------+--------+--------+--------+--------+
         Prior Training  I      1 I      2 I      7 I      3 I      8 I
                         I    3.3 I    6.7 I   23.3 I   10.0 I   26.7 I
                         +--------+--------+--------+--------+--------+
      No Prior Training  I     10 I      9 I      9 I      9 I     13 I
                         I   13.5 I   12.2 I   12.2 I   12.2 I   17.6 I
                         +--------+--------+--------+--------+--------+
                 Column        11       11       16       12       21
                  Total      10.6     10.6     15.4     11.5     20.2
```

Table 56 continued

INDEPENDENT VARIABLE: Prior Systems or Audit Training by $ECCTR (tabulating 1) E commerce Controls

```
                  Count  IPassword Trading
                Row pct  I         Partner    Row
INDEPENDENT VARIABLE:    --------+--------+--------+
                         I      5 I      4 I     30
                         I   16.7 I   13.3 I   28.8
                         +--------+--------+
                      3  I     11 I     13 I     74
                         I   14.9 I   17.6 I   71.2
                         +--------+--------+
                 Column        16       17      104
                  Total      15.4     16.3    100.0
```

Table 57

INDEPENDENT VARIABLE: Graduate Program by Internet Controls

```
               Count   IFirewall Password Satisfac 1x Tokens
INDEPENDENT VARIABLE:  +--------+--------+--------+--------+
                  IM   I      4 I      5 I      0 I      1 I    10
                       I   40.0 I   50.0 I     .0 I   10.0 I  20.8
                       +--------+--------+--------+--------+
               Audit   I      1 I      1 I      0 I      0 I     2
                       I   50.0 I   50.0 I     .0 I     .0 I   4.2
                       +--------+--------+--------+--------+
                Acct   I     11 I     12 I      4 I      4 I    31
                       I   35.5 I   38.7 I   12.9 I   12.9 I  64.6
                       +--------+--------+--------+--------+
               Other   I      2 I      1 I      1 I      1 I     5
                       I   40.0 I   20.0 I   20.0 I   20.0 I  10.4
                       +--------+--------+--------+--------+
              Column         18       19        5        6      48
               Total       37.5     39.6     10.4     12.5   100.0
```

Table 58

INDEPENDENT VARIABLE: Graduate Program by $ECCTR (tabulating 1) E commerce Controls

```
    Count  IApplicat Control  Encrypt  Function Message
  Row pct  Iack      Totals            Ack      Authent
           +--------+--------+--------+--------+--------+
        1  I      5 I      3 I      3 I      4 I      5 I
           I   17.2 I   10.3 I   10.3 I   13.8 I   17.2 I
           +--------+--------+--------+--------+--------+
        2  I      1 I      1 I      1 I      1 I      1 I
           I   14.3 I   14.3 I   14.3 I   14.3 I   14.3 I
           +--------+--------+--------+--------+--------+
        3  I      5 I      7 I     10 I      6 I     13 I
           I    8.1 I   11.3 I   16.1 I    9.7 I   21.0 I
           +--------+--------+--------+--------+--------+
        4  I      0 I      0 I      2 I      1 I      2 I
           I     .0 I     .0 I   33.3 I   16.7 I   33.3 I
           +--------+--------+--------+--------+--------+
   Column        11       11       16       12       21
    Total      10.6     10.6     15.4     11.5     20.2
```

Table 58 continued

INDEPENDENT VARIABLE: Graduate Program by $ECCTR (tabulating 1) E commerce Controls

```
                    Count  IPassword Trading Partners

INDEPENDENT VARIABLE:  +--------+--------+
                    1  I     4  I     5  I    29
                       I  13.8  I  17.2  I  27.9
                       +--------+--------+
                    2  I     1  I     1  I     7
                       I  14.3  I  14.3  I   6.7
                       +--------+--------+
                    3  I    11  I    10  I    62
                       I  17.7  I  16.1  I  59.6
                       +--------+--------+
                    4  I     0  I     1  I     6
                       I    .0  I  16.7  I   5.8
                       +--------+--------+
                  Column     16       17      104
                   Total   15.4     16.3    100.0
```

Table 59

INDEPENDENT VARIABLE: Undergraduate Education by $INTCTR (tabulating 1) Internet Controls

```
                   Count  IFirewall Password Satisfac  1x Token

INDEPENDENT VARIABLE:  +--------+--------+--------+--------+
                    1  I     2  I     3  I     0  I     0  I     5
  Liberal Arts         I  40.0  I  60.0  I    .0  I    .0  I  10.4
                       +--------+--------+--------+--------+
                    2  I     9  I    10  I     4  I     3  I    26
  Business             I  34.6  I  38.5  I  15.4  I  11.5  I  54.2
                       +--------+--------+--------+--------+
                    3  I     7  I     6  I     1  I     3  I    17
  Enginnering/Sciences I  41.2  I  35.3  I   5.9  I  17.6  I  35.4
                       +--------+--------+--------+--------+
                  Column     18       19        5        6      48
                   Total   37.5     39.6     10.4     12.5   100.0
```

Table 60

INDEPENDENT VARIABLE: Undergraduate Education
by $ECCTR (tabulating 1) E commerce Controls

```
                     Count  IApplicat Control  Encrypt  Function Message
                   Row pct  IAck      Totals            Ackn     Authent
INDEPENDENT VARIABLE:       +--------+--------+--------+--------+--------+
                         1  I      2 I      1 I      2 I      2 I      3 I
  Liberal Arts              I  12.5  I   6.3  I  12.5  I  12.5  I  18.8  I
                            +--------+--------+--------+--------+--------+
                         2  I      5 I      6 I      8 I      6 I     11 I
Business                 I   9.6  I  11.5  I  15.4  I  11.5  I  21.2  I
                            +--------+--------+--------+--------+--------+
                         3  I      4 I      4 I      6 I      4 I      7 I
  Enginnering/Sciences      I  11.1  I  11.1  I  16.7  I  11.1  I  19.4  I
                            +--------+--------+--------+--------+--------+
                    Column        11       11       16       12       21
                     Total      10.6     10.6     15.4     11.5     20.2
```

Table 60 continued

INDEPENDENT VARIABLE: Undergraduate Education
by $ECCTR (tabulating 1) E commerce Controls

```
                     Count  IPassword Trading
                   Row pct  I         Partner    Row
INDEPENDENT VARIABLE:       +--------+--------+
                         1  I      3 I      3 I    16
  Liberal Arts              I  18.8  I  18.8  I  15.4
                            +--------+--------+
                         2  I      8 I      8 I    52
  Business                  I  15.4  I  15.4  I  50.0
                            +--------+--------+
                         3  I      5 I      6 I    36
  Enginnering/Sciences      I  13.9  I  16.7  I  34.6
                            +--------+--------+
                    Column        16       17     104
                     Total      15.4     16.3   100.0
```

Table 61

INDEPENDENT VARIABLE: Work Experience by $INTCTR (tabulating 1) Internet Controls

```
                  Count   IFirewall Password Satisfac 1x token
INDEPENDENT VARIABLE:    +--------+--------+--------+--------+
     None                I      5 I      7 I      3 I      2 I     17
                         I   29.4 I   41.2 I   17.6 I   11.8 I   35.4
                         +--------+--------+--------+--------+
     1- 2 Years          I      4 I      3 I      2 I      3 I     12
                         I   33.3 I   25.0 I   16.7 I   25.0 I   25.0
                         +--------+--------+--------+--------+
     3- 5 Years          I      3 I      3 I      0 I      0 I      6
                         I   50.0 I   50.0 I     .0 I     .0 I   12.5
                         +--------+--------+--------+--------+
     5 - 10 Years        I      1 I      1 I      0 I      0 I      2
                         I   50.0 I   50.0 I     .0 I     .0 I    4.2
                         +--------+--------+--------+--------+
     10+ Years           I      5 I      5 I      0 I      1 I     11
                         I   45.5 I   45.5 I     .0 I    9.1 I   22.9
                         +--------+--------+--------+--------+
                 Column        18       19        5        6       48
                  Total      37.5     39.6     10.4     12.5    100.0
```

Table 62

INDEPENDENT VARIABLE: Work Experience by $ECCTR (tabulating 1) E commerce Controls

```
          Count  IApplicat Control   Encrypt  Function Message
        Row pctI           Totals             Acknow   Authent
INDEPENDENT
VARIABLE:       +--------+--------+--------+--------+--------+
              1 I      3 I      4 I      6 I      2 I      8 I    34
                I    8.8 I   11.8 I   17.6 I    5.9 I   23.5 I  32.7
                +--------+--------+--------+--------+--------+
              2 I      1 I      2 I      4 I      3 I      4 I    20
                I    5.0 I   10.0 I   20.0 I   15.0 I   20.0 I  19.2
                +--------+--------+--------+--------+--------+
              3 I      3 I      2 I      1 I      3 I      3 I    17
                I   17.6 I   11.8 I    5.9 I   17.6 I   17.6 I  16.3
                +--------+--------+--------+--------+--------+
              4 I      1 I      0 I      0 I      0 I      1 I     4
                I   25.0 I     .0 I     .0 I     .0 I   25.0 I   3.8
                +--------+--------+--------+--------+--------+
              5 I      3 I      3 I      5 I      4 I      5 I    29
                I   10.3 I   10.3 I   17.2 I   13.8 I   17.2 I  27.9
                +--------+--------+--------+--------+--------+
         Column       11       11       16       12       21
          Total     10.6     10.6     15.4     11.5     20.2
```

Table 62 continued

```
                   Count  IPassword Trading
                 Row pct  I         Partner     Row
INDEPENDENT VARIABLE:     +--------+--------+
                        1 I      6 I      5 I    34
                          I   17.6 I   14.7 I  32.7
                          +--------+--------+
                        2 I      3 I      3 I    20
                          I   15.0 I   15.0 I  19.2
                          +--------+--------+
                        3 I      2 I      3 I    17
                          I   11.8 I   17.6 I  16.3
                          +--------+--------+
                        4 I      1 I      1 I     4
                          I   25.0 I   25.0 I   3.8
                          +--------+--------+
                        5 I      4 I      5 I    29
                          I   13.8 I   17.2 I  27.9
                          +--------+--------+
                  Column        16       17     104
                   Total      15.4     16.3   100.0
```

Table 63

Is a business continuity plan important within an organization

25	N	%
Yes	25	100%

Table 64

Which of the Following should be in a Business Continuity Planning within an Organization?

	N	**%**
no formal business continuity plan	0	0%
end user computing	18	72%
mission critical	23	92%
complete restoration	13	52%
enterprise network	21	84%
LANs	20	80%
Operations Center	19	76%

Table 65

***** CROSSTABULATION *****
INDEPENDENT VARIABLE: Computer Proficiency
by $BCP (tabulating 1) Include in BCP

```
                  Count  IEnd user Enterpri  Operation LANS    Recovery
                Row pct  Icomputing SNetworks
INDEPENDENT VARIABLE:    +--------+--------+--------+--------+--------+
                 Expert  I     4  I     6  I     5  I     6  I     6  I
                         I  13.3  I  20.0  I  16.7  I  20.0  I  20.0  I
                         +--------+--------+--------+--------+--------+
           Intermediate  I    12  I    12  I    12  I    11  I    14  I
                         I  17.1  I  17.1  I  17.1  I  15.7  I  20.0  I
                         +--------+--------+--------+--------+--------+
                 Novice  I     2  I     3  I     3  I     2  I     3  I
                         I  14.3  I  21.4  I  21.4  I  14.3  I  21.4  I
                         +--------+--------+--------+--------+--------+
                 Column       18       21       20       19       23
                  Total     15.8     18.4     17.5     16.7     20.2
```

Table 67

***** CROSSTABULATION *****
INDEPENDENT VARIABLE: InfoProfessional
by $BCP (tabulating 1) Include in BCP

```
                         I End User Network  LANS     Ops      Recovery
INDEPENDENT VARIABLE:     --------+--------+--------+--------+--------+
                      1  I     8  I    12  I    10  I     9  I    12  I
  Information/Audit Pr   I  14.3  I  21.4  I  17.9  I  16.1  I  21.4  I
                         +--------+--------+--------+--------+--------+
                      2  I     4  I     4  I     5  I     5  I     5  I
  Not an Information/A   I  14.8  I  14.8  I  18.5  I  18.5  I  18.5  I
                         +--------+--------+--------+--------+--------+
                      3  I     6  I     5  I     5  I     5  I     6  I
  Do Not Know            I  19.4  I  16.1  I  16.1  I  16.1  I  19.4  I
                         +--------+--------+--------+--------+--------+
                 Column       18       21       20       19       23
                  Total     15.8     18.4     17.5     16.7     20.2
```

Table 67 continued

***** CROSSTABULATION *****
INDEPENDENT VARIABLE: InfoProfessional
by $BCP (tabulating 1) Include in BCP

```
                    Complete
                    Restoration
INDEPENDENT VARIABLE  +--------+
                   1  I      5  I    56
  Information/Audit Pr I   8.9  I   49.1
                      +--------+
                   2  I      4  I    27
  Not an Information/A I  14.8  I   23.7
                      +--------+
                   3  I      4  I    31
  Do Not Know          I  12.9  I   27.2
                      +--------+
              Column        13      114
               Total      11.4    100.0
```

Table 68

***** CROSSTABULATION *****
INDEPENDENT VARIABLE: Major Concentration
by $BCP (tabulating 1) Include in BCP

```
                Count  Iend user Enterpri          Operatio Recovery
              Row pct  Icomputing           network Center   mission
INDEPENDENT VARIABLE:  +--------+--------+--------+--------+--------+
                    1  I      8  I     11  I     10  I     10  I     11  I
                       I   14.5  I   20.0  I   18.2  I   18.2  I   20.0  I
                       +--------+--------+--------+--------+--------+
                    2  I      3  I      4  I      3  I      2  I      5  I
                       I   15.8  I   21.1  I   15.8  I   10.5  I   26.3  I
                       +--------+--------+--------+--------+--------+
                    4  I      4  I      2  I      4  I      3  I      3  I
                       I   21.1  I   10.5  I   21.1  I   15.8  I   15.8  I
                       +--------+--------+--------+--------+--------+
                    6  I      1  I      1  I      1  I      1  I      1  I
                       I   16.7  I   16.7  I   16.7  I   16.7  I   16.7  I
                       +--------+--------+--------+--------+--------+
                    7  I      2  I      3  I      2  I      3  I      3  I
                       I   13.3  I   20.0  I   13.3  I   20.0  I   20.0  I
                       +--------+--------+--------+--------+--------+
               Column        18        21        20        19        23
                Total      15.8      18.4      17.5      16.7      20.2
```

Table 68 continued

* * * CROSSTABULATION * * *

INDEPENDENT VARIABLE: Major Concentration
by $BCP (tabulating 1) Include in BCP

```
                 Count  IComplete
               Row pct  Irestoration  Row
                                      Total
INDEPENDENT VARIABLE:   +--------+
                     1  I     5  I    55
                        I   9.1  I  48.2
                        +--------+
                     2  I     2  I    19
                        I  10.5  I  16.7
                        +--------+
                     4  I     3  I    19
                        I  15.8  I  16.7
                        +--------+
                     6  I     1  I     6
                        I  16.7  I   5.3
                        +--------+
                     7  I     2  I    15
                        I  13.3  I  13.2
                        +--------+
                Column       13      114
                 Total     11.4    100.0
```

Table 69

INDEPENDENT VARIABLE: Prior Systems or Audit Training
by $BCP (tabulating 1) Include in BCP

```
                 Count  Iend user enterpri          Operatio Recovery
               Row pct  Icomputi           networks Center
INDEPENDENT VARIABLE:   +--------+--------+--------+--------+--------+
                     2  I     5  I     8  I     8  I     9  I     9  I
                        I  11.9  I  19.0  I  19.0  I  21.4  I  21.4  I
                        +--------+--------+--------+--------+--------+
                     3  I    13  I    13  I    12  I    10  I    14  I
                        I  18.1  I  18.1  I  16.7  I  13.9  I  19.4  I
                        +--------+--------+--------+--------+--------+
                Column       18       21       20       19       23
                 Total     15.8     18.4     17.5     16.7     20.2
```

Table 69 continued

*** CROSSTABULATION ***

INDEPENDENT VARIABLE: Prior Systems or Audit Training by $BCP (tabulating 1) Include in BCP

```
                  Count   Icomplete
                 Row pct  Irestoration Row
                          Ition        Total
INDEPENDENT VARIABLE:     +--------+
                       2  I     3  I    42
                          I   7.1  I  36.8
                          +--------+
                       3  I    10  I    72
                          I  13.9  I  63.2
                          +--------+
                 Column       13       114
                  Total     11.4     100.0
```

Table 70

*** CROSSTABULATION ***

INDEPENDENT VARIABLE: Graduate Program by $BCP (tabulating 1) Include in BCP

```
                 Count   IEnd user Enterprise        Operations Recovery
                Row pct  IComputing           LANS              Mission
INDEPENDENT VARIABLE:    +--------+--------+--------+--------+--------+
                      1  I     4  I     3  I     4  I     3  I     4  I
  MBA                    I  18.2  I  13.6  I  18.2  I  13.6  I  18.2  I
                         +--------+--------+--------+--------+--------+
                      2  I     1  I     1  I     1  I     1  I     1  I
  Ph.D                   I  20.0  I  20.0  I  20.0  I  20.0  I  20.0  I
                         +--------+--------+--------+--------+--------+
                      3  I    11  I    15  I    12  I    12  I    16  I
  MPA                    I  15.1  I  20.5  I  16.4  I  16.4  I  21.9  I
                         +--------+--------+--------+--------+--------+
                      4  I     2  I     2  I     3  I     3  I     2  I
  PPA                    I  14.3  I  14.3  I  21.4  I  21.4  I  14.3  I
                         +--------+--------+--------+--------+--------+
                Column       18       21       20       19       23
                 Total     15.8     18.4     17.5     16.7     20.2
```

Table 70 continued

***** CROSSTABULATION *****
INDEPENDENT VARIABLE: Graduate Program
by $BCP (tabulating 1) Include in BCP

```
                  Count  Icomplete
                Row pct  Irestoration Row
                                      Total
INDEPENDENT VARIABLE:    +--------+
                      1  I     4  I    22
  MBA                    I  18.2  I  19.3
                         +--------+
                      2  I     0  I     5
  Ph.D                   I    .0  I   4.4
                         +--------+
                      3  I     7  I    73
  MPA                    I   9.6  I  64.0
                         +--------+
                      4  I     2  I    14
  PPA                    I  14.3  I  12.3
                         +--------+
                 Column       13      114
                  Total     11.4    100.0
```

Table 71

*** CROSSTABULATION ***
INDEPENDENT VARIABLE: Undergrad Education
by $BCP (tabulating 1) Include in BCP

```
                   Count  I End user Enterprise      Operations
                 Row pct  IComputing         LANS
INDEPENDENT VARIABLE:    +--------+--------+--------+--------+
                       1 I     3  I     3  I     3  I     3  I
                         I  16.7  I  16.7  I  16.7  I  16.7  I
                         +--------+--------+--------+--------+
                       2 I     9  I    11  I    10  I     9  I
                         I  16.1  I  19.6  I  17.9  I  16.1  I
                         +--------+--------+--------+--------+
                       3 I     6  I     7  I     7  I     7  I
                         I  15.0  I  17.5  I  17.5  I  17.5  I
                         +--------+--------+--------+--------+
                  Column       18       21       20       19
                   Total     15.8     18.4     17.5     16.7
```

Table 71 continued

*** CROSSTABULATION ***
INDEPENDENT VARIABLE: Undergrad Education
by $BCP (tabulating 1) Include in BCP

```
                   Count  IComplete
                 Row pct  Irestoration Row

INDEPENDENT VARIABLE:    +--------+
                       1 I     3  I    18
                         I  16.7  I  15.8
                         +--------+
                       2 I     4  I    56
                         I   7.1  I  49.1
                         +--------+
                       3 I     6  I    40
                         I  15.0  I  35.1
                         +--------+
                  Column       13     114
                   Total     11.4   100.0
```

Table 72

***** CROSSTABULATION *****
INDEPENDENT VARIABLE: Work Experience
by $BCP (tabulating 1) Include in BCP

```
                    Count  Iend user enterpri         Operations recovery
                  Row pct  Icomputi          LANS
INDEPENDENT VARIABLE:      +--------+--------+--------+--------+--------+
                        1  I      6 I      8 I      8 I      6 I      9 I
  None                     I   14.3 I   19.0 I   19.0 I   14.3 I   21.4 I
                           +--------+--------+--------+--------+--------+
                        2  I      4 I      4 I      5 I      5 I      4 I
  1 - 2 years              I   16.0 I   16.0 I   20.0 I   20.0 I   16.0 I
                           +--------+--------+--------+--------+--------+
                        3  I      2 I      3 I      2 I      2 I      3 I
  3 - 5 years              I   15.4 I   23.1 I   15.4 I   15.4 I   23.1 I
                           +--------+--------+--------+--------+--------+
                        4  I      1 I      1 I      1 I      1 I      1 I
  5 -10 years              I   16.7 I   16.7 I   16.7 I   16.7 I   16.7 I
                           +--------+--------+--------+--------+--------+
                        5  I      5 I      5 I      4 I      5 I      6 I
  10+ years                I   17.9 I   17.9 I   14.3 I   17.9 I   21.4 I
                           +--------+--------+--------+--------+--------+
                   Column        18       21       20       19       23
                    Total      15.8     18.4     17.5     16.7     20.2
```

Table 72 continued

```
                      * * *  C R O S S T A B U L A T I O N  * * *

                        INDEPENDENT VARIABLE:  Work Experience
                        by $BCP (tabulating 1)  Include in BCP

                         Count   IComplete
                        Row pct  IRestoration  Row

INDEPENDENT VARIABLE:   +---------+
                      1  I      5  I     42
  None                   I   11.9  I   36.8
                         +---------+
                      2  I      3  I     25
  1 - 2 years            I   12.0  I   21.9
                         +---------+
                      3  I      1  I     13
  3 - 5 years            I    7.7  I   11.4
                         +---------+
                      4  I      1  I      6
  5 -10 years            I   16.7  I    5.3
                         +---------+
                      5  I      3  I     28
  10+ years              I   10.7  I   24.6
                         +---------+
                 Column        13        114
                  Total      11.4      100.0
```

Table 73

Which of the following should be included in a company's formal corporate information/data security policy?

	n	%
Incident response and reporting	19	76%
Centralized security administration	18	72%
Records management	18	72%
External access	17	68%
End user computing	17	68%
Data classification	16	64%
Personnel security non disclosure agreements	16	64%
Surveillance and monitoring	16	64%
Business continuity planning corporate wide	15	60%
Electronic commerce services	12	48%
None of the above / no formal policy	1	4%

Table 74

Does an Organization need a Stand Alone Information Policy

Responses	25	%	Cum %
Yes	23	92%	92%
No	2	8%	100%

Table 75

Should an Organization Implement Security Measures on all Systems and Information?

	N	%
Yes	19	76%
No	6	24%

Table 76

Where does an organization's most dangerous security threat come from?

	n	%
from outside an organization	5	20%
from inside an organization	20	80%

Table 77

What are the key security issues that concern you?

Information Security	n	%
Internet Security	17	68%
Intranet Security	19	76%
Virus Infection	16	64%
Access Control	10	40%
Firewalls	10	40%
Communications Security	7	28%

Business Security		
E commerce	16	64%
Remote Access	10	40%
Software Licensing	3	12%
Security Administration	11	44%
Disaster	18	72%
Year 2000	17	68%
Training	12	48%
Industrial Espionage	12	48%

Table 78

How frequently do you want/need information on key security concerns

Count	**n**	%	Cum %
Monthly	18	72%	72%
Bimonthly	2	8%	80%
quarterly	4	16%	96%
annually	1	4%	100%
never	0	0%	100%

Table 79

Do you feel it is important for senior management to be involved in information and data security

		Not		**Somewhat**				**Extremely**	
		Imp		**Important**		**Important**		**Important**	
Head of Info Systems	25			1	4%	6	24%	18	72%
IS Department Head	21			3	14%	8	38%	10	48%
Non IS Executive	22	1	5%	7	32%		0%	2	9%
Internal audit	21			3	14%	9	43%	9	43%
Other	9	2	22%	3	33%	2	22%	2	22%

Table 80

Crosstabulation
INDEPENDENT VARIABLE: Computer Proficiency
by $SRMGT (group) Senior Management Involvement

```
                      Count   INot Imp Somewhat Important Extremely
                    Row pct I         Important          Important    Row

INDEPENDENT VARIABLE:       +--------+--------+--------+--------+
                          2 I      1 I      5 I     10 I      9 I     25
  Expert                    I   4.0  I  20.0  I  40.0  I  36.0  I   25.8
                            +--------+--------+--------+--------+
                          3 I      2 I     12 I     23 I     25 I     62
  Intermediate              I   3.2  I  19.4  I  37.1  I  40.3  I   63.9
                            +--------+--------+--------+--------+
                          4 I      0 I      0 I      3 I      7 I     10
  Novice                    I    .0  I    .0  I  30.0  I  70.0  I   10.3
                            +--------+--------+--------+--------+
                    Column         3       17       36       41       97
                     Total       3.1     17.5     37.1     42.3    100.0
```

Table 81

*** * * CROSSTABULATION * * ***

INDEPENDENT VARIABLE: Computer Proficiency
by $ISKEY (tabulating 1) Key Issues

```
                      Count  IInternet Intranet Virus In Access   Firewalls
                    Row pct ISecurity Securit          Control
INDEPENDENT VARIABLE:       +--------+--------+--------+--------+--------+
                          2 I      4 I      3 I      4 I      3 I      4 I
  Expert                    I  17.4  I  13.0  I  17.4  I  13.0  I  17.4  I
                            +--------+--------+--------+--------+--------+
                          3 I     10 I     13 I      8 I      5 I      4 I
  Intermediate              I  20.4  I  26.5  I  16.3  I  10.2  I   8.2  I
                            +--------+--------+--------+--------+--------+
                          4 I      2 I      2 I      3 I      1 I      1 I
  Novice                    I  20.0  I  20.0  I  30.0  I  10.0  I  10.0  I
                            +--------+--------+--------+--------+--------+
                    Column        16       18       15        9        9
                     Total      19.5     22.0     18.3     11.0     11.0
```

Table 81 continued

*** CROSSTABULATION ***
INDEPENDENT VARIABLE: Computer Proficiency
by $ISKEY (tabulating 1) Key Issues

```
                  Count   ICommunic Biometric Computer Other se
                Row pct   I                   Security   Row
INDEPENDENT VARIABLE:     +--------+--------+--------+--------+
                      2   I      1  I      3  I      1  I      0  I     23
  Expert                  I    4.3  I   13.0  I    4.3  I     .0  I   28.0
                          +--------+--------+--------+--------+
                      3   I      4  I      1  I      3  I      1  I     49
  Intermediate            I    8.2  I    2.0  I    6.1  I    2.0  I   59.8
                          +--------+--------+--------+--------+
                      4   I      1  I      0  I      0  I      0  I     10
  Novice                  I   10.0  I     .0  I     .0  I     .0  I   12.2
                          +--------+--------+--------+--------+
                Column          6         4         4         1        82
                 Total        7.3       4.9       4.9       1.2     100.0
```

Table 82

*** CROSSTABULATION ***

INDEPENDENT VARIABLE: Computer Proficiency
by $BUSSEC (tabulating 1) Key Issues Business Security

```
                  Count   IDisaster Ecomm   Indust.   Info   Remote Access
                Row pct   IRecovery          Espio    Secur  ccess        Row

INDEPENDENT VARIABLE:     +--------+--------+--------+--------+--------+
                      2   I      3  I      1  I      5  I      4  I      2  I
  Expert                  I   14.3  I    4.8  I   23.8  I   19.0  I    9.5  I
                          +--------+--------+--------+--------+--------+
                      3   I     11  I     11  I      5  I     12  I      6  I
  Intermediate            I   15.5  I   15.5  I    7.0  I   16.9  I    8.5  I
                          +--------+--------+--------+--------+--------+
                      4   I      3  I      3  I      1  I      2  I      1  I
  Novice                  I   17.6  I   17.6  I    5.9  I   11.8  I    5.9  I
                          +--------+--------+--------+--------+--------+
                Column         17        15        11        18         9
                 Total       15.6      13.8      10.1      16.5       8.3
```

Table 82 continued

*** CROSSTABULATION ***
INDEPENDENT VARIABLE: Computer Proficiency
by $BUSSEC (tabulating 1) Key Issues Business Security

```
                   Count  ISecurity Software Training Year 2000
INDEPENDENT VARIABLE      +--------+--------+--------+--------+
                          I      1 I      0 I      2 I      3 I    21
 Expert                   I    4.8 I     .0 I    9.5 I   14.3 I   19.3
                          +--------+--------+--------+--------+
                          I      7 I      1 I      8 I     10 I    71
 Intermediate             I    9.9 I    1.4 I   11.3 I   14.1 I   65.1
                          +--------+--------+--------+--------+
                          I      2 I      1 I      1 I      3 I    17
 Novice                   I   11.8 I    5.9 I    5.9 I   17.6 I   15.6
                          +--------+--------+--------+--------+
                  Column        10        2       11       16      109
                   Total       9.2      1.8     10.1     14.7    100.0
```

Table 83

INDEPENDENT VARIABLE: Computer Proficiency
by $CORPPOL (tabulating 1) Formal Security Policy

```
                   Count  ICentral  Data     External Ecommerce Incident
                 Row pct  ISecurity Class    Access             Response
INDEPENDENT VARIABLE:     +--------+--------+--------+--------+--------+
                          I      5 I      4 I      4 I      2 I      5 I
 Expert                   I   14.7 I   11.8 I   11.8 I    5.9 I   14.7 I
                          +--------+--------+--------+--------+--------+
                          I     11 I     10 I     10 I      8 I     11 I
 Intermediate             I   11.3 I   10.3 I   10.3 I    8.2 I   11.3 I
                          +--------+--------+--------+--------+--------+
                          I      2 I      1 I      2 I      1 I      2 I
 Novice                   I   13.3 I    6.7 I   13.3 I    6.7 I   13.3 I
                          +--------+--------+--------+--------+--------+
                  Column        18       15       16       11       18
                   Total      12.3     10.3     11.0      7.5     12.3
```

Table 83 continued

INDEPENDENT VARIABLE: Computer Proficiency
by $CORPPOL (tabulating 1) Formal Security Policy

```
                       Count   IPersonne Records  Surveill Organiza End user
                     Row pct   Il securi manageme ance and tion Most Computing
INDEPENDENT VARIABLE:          +--------+--------+--------+--------+--------+
                           2   I      4  I      4  I      3  I      0  I      3  I
  Expert                       I   11.8  I   11.8  I    8.8  I     .0  I    8.8  I
                               +--------+--------+--------+--------+--------+
                           3   I      9  I     11  I     11  I      4  I     12  I
  Intermediate                 I    9.3  I   11.3  I   11.3  I    4.1  I   12.4  I
                               +--------+--------+--------+--------+--------+
                           4   I      2  I      2  I      1  I      1  I      1  I
  Novice                       I   13.3  I   13.3  I    6.7  I    6.7  I    6.7  I
                               +--------+--------+--------+--------+--------+
                      Column         15        17        15         5        16
                       Total       10.3      11.6      10.3       3.4      11.0
```

Table 84

* * * CROSSTABULATION * * *
INDEPENDENT VARIABLE: InfoProfessional
by $SRMGT (group) Senior Management Involvement

```
                       Count   INot Imp Somewhat Important Extreme
                     Row pct   Irtant   Important          Imporant    Row
                               I     1  I     2  I     3  I     4  I
INDEPENDENT VARIABLE:          +--------+--------+--------+--------+
                           1   I      0  I      8  I     17  I     18  I     43
  Information/Audit Pr         I     .0  I   18.6  I   39.5  I   41.9  I   44.3
                               +--------+--------+--------+--------+
                           2   I      2  I      3  I     10  I      9  I     24
  Not an Information/A         I    8.3  I   12.5  I   41.7  I   37.5  I   24.7
                               +--------+--------+--------+--------+
                           3   I      1  I      6  I      9  I     14  I     30
  Do Not Know                  I    3.3  I   20.0  I   30.0  I   46.7  I   30.9
                               +--------+--------+--------+--------+
                      Column          3        17        36        41        97
                       Total        3.1      17.5      37.1      42.3     100.0
```

Table 85

*** C R O S S T A B U L A T I O N ***
INDEPENDENT VARIABLE: InfoProfessional
by $ISKEY (tabulating 1) Key Issues

```
                   Count  IInternet Intranet Virus   Access   Firewalls
                 Row pct  ISecurit  Security         Control
INDEPENDENT VARIABLE:    +--------+--------+--------+--------+--------+
                       1  I     8  I     8  I    10  I     4  I     6  I
   Information/Audit Pr  I  17.8  I  17.8  I  22.2  I   8.9  I  13.3  I
                         +--------+--------+--------+--------+--------+
                       2  I     3  I     4  I     2  I     3  I     1  I
   Not an Information/A  I  20.0  I  26.7  I  13.3  I  20.0  I   6.7  I
                         +--------+--------+--------+--------+--------+
                       3  I     5  I     6  I     3  I     2  I     2  I
   Do Not Know            I  22.7  I  27.3  I  13.6  I   9.1  I   9.1  I
                         +--------+--------+--------+--------+--------+
                 Column        16       18       15        9        9
                  Total      19.5     22.0     18.3     11.0     11.0
```

Table 85 continued

*** C R O S S T A B U L A T I O N ***
INDEPENDENT VARIABLE: InfoProfessional
by $ISKEY (tabulating 1) Key Issues

```
                   Count  ICommunic Biometri Computer Other
                 Row pct  Iations            Forensic Security      Row
INDEPENDENT VARIABLE:    +--------+--------+--------+--------+
                       1  I     4  I     4  I     1  I     0  I      45
   Information/Audit Pr  I   8.9  I   8.9  I   2.2  I    .0  I    54.9
                         +--------+--------+--------+--------+
                       2  I     1  I     0  I     1  I     0  I      15
   Not an Information/A  I   6.7  I    .0  I   6.7  I    .0  I    18.3
                         +--------+--------+--------+--------+
                       3  I     1  I     0  I     2  I     1  I      22
   Do Not Know            I   4.5  I    .0  I   9.1  I   4.5  I    26.8
                         +--------+--------+--------+--------+
                 Column         6        4        4        1       82
                  Total       7.3      4.9      4.9      1.2    100.0
```

Table 86

*** CROSSTABULATION ***
INDEPENDENT VARIABLE: InfoProfessional
by $BUSSEC (tabulating 1) Key Issues Business Security

```
                    Count  IDisaster Ecomm  Industri Info on  Remote
                  Row pct  IRecover          Esp     Security Access Total

INDEPENDENT VARIABLE:      +--------+--------+--------+--------+--------+
                        1  I    10  I     4  I     6  I     9  I     3  I
     Information/Audit Pr  I  20.0  I   8.0  I  12.0  I  18.0  I   6.0  I
                           +--------+--------+--------+--------+--------+
                        2  I     2  I     5  I     1  I     4  I     3  I
     Not an Information/A  I   8.7  I  21.7  I   4.3  I  17.4  I  13.0  I
                           +--------+--------+--------+--------+--------+
                        3  I     5  I     6  I     4  I     5  I     3  I
     Do Not Know           I  13.9  I  16.7  I  11.1  I  13.9  I   8.3  I
                           +--------+--------+--------+--------+--------+
                   Column       17       15       11       18        9
                    Total     15.6     13.8     10.1     16.5      8.3
```

Table 86 continued

*** CROSSTABULATION ***
INDEPENDENT VARIABLE: InfoProfessional
by $BUSSEC (tabulating 1) Key Issues Business Security

```
                    Count  ISecurity Software Training Year 2000
INDEPENDENT VARIABLE:      +--------+--------+--------+--------+
                        1  I     5  I     1  I     5  I     7  I     50
     Information/Audit Pr  I  10.0  I   2.0  I  10.0  I  14.0  I   45.9
                           +--------+--------+--------+--------+
                        2  I     2  I     0  I     2  I     4  I     23
     Not an Information/A  I   8.7  I    .0  I   8.7  I  17.4  I   21.1
                           +--------+--------+--------+--------+
                        3  I     3  I     1  I     4  I     5  I     36
     Do Not Know           I   8.3  I   2.8  I  11.1  I  13.9  I   33.0
                           +--------+--------+--------+--------+
                   Column       10        2       11       16      109
                    Total      9.2      1.8     10.1     14.7    100.0
```

Table 87

***** CROSSTABULATION *****
INDEPENDENT VARIABLE: InfoProfessional
by $CORPPOL (tabulating 1) Formal Security Policy

```
                 Count  ICentrali Data     External Ecommerce Incident
               Row pct  ISecurity Class    Access             Response
INDEPENDENT VARIABLE:   +--------+--------+--------+--------+--------+
                    1   I    11  I    10  I    10  I     6  I    10  I
  Information/Audit Pr  I  12.8  I  11.6  I  11.6  I   7.0  I  11.6  I
                        +--------+--------+--------+--------+--------+
                    2   I     3  I     2  I     2  I     3  I     4  I
  Not an Information/A  I  12.5  I   8.3  I   8.3  I  12.5  I  16.7  I
                        +--------+--------+--------+--------+--------+
                    3   I     4  I     3  I     4  I     2  I     4  I
  Do Not Know           I  11.1  I   8.3  I  11.1  I   5.6  I  11.1  I
                        +--------+--------+--------+--------+--------+
                Column       18       15       16       11       18
                 Total     12.3     10.3     11.0      7.5     12.3
```

Table 87 continued

***** CROSSTABULATION *****
INDEPENDENT VARIABLE: InfoProfessional
by $CORPPOL (tabulating 1) Formal Security Policy

```
                 Count  IPersonnel Records  Surveill Organiza End user
               Row pct   securi    manage                     computing

INDEPENDENT VARIABLE:   +--------+--------+--------+--------+--------+
                    1   I    10  I    11  I     9  I     0  I     9  I
  Information/Audit Pr  I  11.6  I  12.8  I  10.5  I    .0  I  10.5  I
                        +--------+--------+--------+--------+--------+
                    2   I     2  I     2  I     2  I     2  I     2  I
  Not an Information/A  I   8.3  I   8.3  I   8.3  I   8.3  I   8.3  I
                        +--------+--------+--------+--------+--------+
                    3   I     3  I     4  I     4  I     3  I     5  I
  Do Not Know           I   8.3  I  11.1  I  11.1  I   8.3  I  13.9  I
                        +--------+--------+--------+--------+--------+
                Column       15       17       15        5       16
                 Total     10.3     11.6     10.3      3.4     11.0
```

Table 88

* * * CROSSTABULATION * * *
INDEPENDENT VARIABLE: Major Concentration
By Senior Management Involvement

```
                     Count  INot Imp  Somewhat  Import   Extreme  IMP
INDEPENDENT VARIABLE:       +--------+--------+--------+--------+
                         1  I      1 I      8 I     16 I     17 I     42
  Information Manageme      I    2.4 I   19.0 I   38.1 I   40.5 I   43.3
                            +--------+--------+--------+--------+
                         2  I      1 I      5 I      9 I      6 I     21
  Audit                     I    4.8 I   23.8 I   42.9 I   28.6 I   21.6
                            +--------+--------+--------+--------+
                         4  I      0 I      2 I      4 I     11 I     17
  Accounting                I     .0 I   11.8 I   23.5 I   64.7 I   17.5
                            +--------+--------+--------+--------+
                         6  I      0 I      0 I      2 I      2 I      4
  Management                I     .0 I     .0 I   50.0 I   50.0 I    4.1
                            +--------+--------+--------+--------+
                         7  I      1 I      2 I      5 I      5 I     13
  Other                     I    7.7 I   15.4 I   38.5 I   38.5 I   13.4
                            +--------+--------+--------+--------+
                    Column         3       17       36       41      97
                     Total       3.1     17.5     37.1     42.3   100.0
```

Table 89

***** CROSSTABULATION *****
INDEPENDENT VARIABLE: Major Concentration
by $ISKEY (tabulating 1) Key Issues

```
                       Count  IInternet Intranet Virus    Access   Firewalls
                     Row pct  ISecurity Security Infection Control
INDEPENDENT VARIABLE: -+--------+--------+--------+--------+--------+
                         1  I     5  I     8  I     6  I     3  I     3  I
  Information Manageme  I  16.7  I  26.7  I  20.0  I  10.0  I  10.0  I
                            +--------+--------+--------+--------+--------+
                         2  I     3  I     3  I     4  I     2  I     2  I
  Audit                     I  17.6  I  17.6  I  23.5  I  11.8  I  11.8  I
                            +--------+--------+--------+--------+--------+
                         4  I     4  I     5  I     2  I     2  I     1  I
  Accounting                I  23.5  I  29.4  I  11.8  I  11.8  I   5.9  I
                            +--------+--------+--------+--------+--------+
                         6  I     1  I     1  I     1  I     1  I     1  I
  Management                I  16.7  I  16.7  I  16.7  I  16.7  I  16.7  I
                            +--------+--------+--------+--------+--------+
                         7  I     3  I     1  I     2  I     1  I     2  I
  Other                     I  25.0  I   8.3  I  16.7  I   8.3  I  16.7  I
                            +--------+--------+--------+--------+--------+
                    Column        16       18       15        9        9
                     Total      19.5     22.0     18.3     11.0     11.0
```

Table 89 continued

***** CROSSTABULATION *****
INDEPENDENT VARIABLE: Major Concentration
by SISKEY (tabulating 1) Key Issues

```
                   Count  ICommunic Biometric Computer Other
                 Row pct  I                   Forensics Security   Row
INDEPENDENT VARIABLE:     +--------+--------+--------+--------+
                       1  I     3  I     2  I     0  I     0  I    30
  Information Manageme    I  10.0  I   6.7  I    .0  I    .0  I  36.6
                          +--------+--------+--------+--------+
                       2  I     0  I     0  I     3  I     0  I    17
  Audit                   I    .0  I    .0  I  17.6  I    .0  I  20.7
                          +--------+--------+--------+--------+
                       4  I     1  I     0  I     1  I     1  I    17
  Accounting              I   5.9  I    .0  I   5.9  I   5.9  I  20.7
                          +--------+--------+--------+--------+
                       6  I     1  I     0  I     0  I     0  I     6
  Management              I  16.7  I    .0  I    .0  I    .0  I   7.3
                          +--------+--------+--------+--------+
                       7  I     1  I     2  I     0  I     0  I    12
  Other                   I   8.3  I  16.7  I    .0  I    .0  I  14.6
                          +--------+--------+--------+--------+
                  Column        6        4        4        1       82
                   Total      7.3      4.9      4.9      1.2    100.0
```

Table 90

***** CROSSTABULATION *****
INDEPENDENT VARIABLE: Major Concentration
by $BUSSEC (tabulating 1) Key Issues Business Security

```
                     Count  IDisaster Ecommerce Indust Info      Remote
                   Row pct  IRecovery            Espio  Security Access
INDEPENDENT VARIABLE:       +--------+--------+--------+--------+--------+
                         1  I      8 I      7 I      4 I      6 I      4 I
  Information Manageme      I  18.6  I  16.3  I   9.3  I  14.0  I   9.3  I
                            +--------+--------+--------+--------+--------+
                         2  I      4 I      1 I      2 I      5 I      1 I
  Audit                     I  18.2  I   4.5  I   9.1  I  22.7  I   4.5  I
                            +--------+--------+--------+--------+--------+
                         4  I      3 I      5 I      3 I      4 I      3 I
  Accounting                I  10.3  I  17.2  I  10.3  I  13.8  I  10.3  I
                            +--------+--------+--------+--------+--------+
                         6  I      1 I      1 I      0 I      1 I      1 I
  Management                I  14.3  I  14.3  I    .0  I  14.3  I  14.3  I
                            +--------+--------+--------+--------+--------+
                         7  I      1 I      1 I      2 I      2 I      0 I
  Other                     I  12.5  I  12.5  I  25.0  I  25.0  I    .0  I
                            +--------+--------+--------+--------+--------+
                    Column        17       15       11       18        9
                     Total      15.6     13.8     10.1     16.5      8.3
```

Table 90 continued

***** CROSSTABULATION *****
INDEPENDENT VARIABLE: Major Concentration
by $BUSSEC (tabulating 1) Key Issues Business Security

```
                        Count  ISecurity Software Training Year 2000
INDEPENDENT VARIABLE:          +--------+--------+--------+--------+
                            1  I      3 I      1 I      3 I      7 I   43
  Information Manageme         I    7.0 I    2.3 I    7.0 I   16.3 I  39.4
                               +--------+--------+--------+--------+
                            2  I      4 I      0 I      3 I      2 I   22
  Audit                        I   18.2 I     .0 I   13.6 I    9.1 I  20.2
                               +--------+--------+--------+--------+
                            4  I      2 I      1 I      3 I      5 I   29
  Accounting                   I    6.9 I    3.4 I   10.3 I   17.2 I  26.6
                               +--------+--------+--------+--------+
                            6  I      1 I      0 I      1 I      1 I    7
  Management                   I   14.3 I     .0 I   14.3 I   14.3 I   6.4
                               +--------+--------+--------+--------+
                            7  I      0 I      0 I      1 I      1 I    8
  Other                        I     .0 I     .0 I   12.5 I   12.5 I   7.3
                               +--------+--------+--------+--------+
                      Column         10        2       11       16     109
                       Total        9.2      1.8     10.1     14.7   100.0
```

Table 91

* * * CROSSTABULATION * * *
INDEPENDENT VARIABLE: Major Concentration
by $CORPPOL (tabulating 1) Formal Security Policy

```
                    Count  ICentral Data      External Electron Incident
                  Row pct  ISecu    Class     Access   Commerce Respons
INDEPENDENT VARIABLE:      +--------+--------+--------+--------+--------+
                        1  I      8 I      7 I      9 I      6 I      9 I
  Information Manageme     I   11.1 I    9.7 I   12.5 I    8.3 I   12.5 I
                           +--------+--------+--------+--------+--------+
                        2  I      4 I      2 I      1 I      0 I      2 I
  Audit                    I   21.1 I   10.5 I    5.3 I     .0 I   10.5 I
                           +--------+--------+--------+--------+--------+
                        4  I      3 I      3 I      3 I      3 I      3 I
  Accounting               I   10.0 I   10.0 I   10.0 I   10.0 I   10.0 I
                           +--------+--------+--------+--------+--------+
                        6  I      1 I      1 I      1 I      1 I      1 I
  Management               I   11.1 I   11.1 I   11.1 I   11.1 I   11.1 I
                           +--------+--------+--------+--------+--------+
                        7  I      2 I      2 I      2 I      1 I      3 I
  Other                    I   12.5 I   12.5 I   12.5 I    6.3 I   18.8 I
                           +--------+--------+--------+--------+--------+
                   Column        18       15       16       11       18
                    Total      12.3     10.3     11.0      7.5     12.3
```

Table 92 continued

*** CROSSTABULATION ***
INDEPENDENT VARIABLE: Major Concentration
by $CORPPOL (tabulating 1) Formal Security Policy

```
                       Count   IPersonne Records  Surveill Organiza End user
                     Row pct   Isecuriyt manage            tion     computing
INDEPENDENT VARIABLE:          +--------+--------+--------+--------+--------+
                           1   I     9  I     8  I     7  I     1  I     8  I
  Information Manageme         I  12.5  I  11.1  I   9.7  I   1.4  I  11.1  I
                               +--------+--------+--------+--------+--------+
                           2   I     1  I     3  I     3  I     0  I     3  I
  Audit                        I   5.3  I  15.8  I  15.8  I    .0  I  15.8  I
                               +--------+--------+--------+--------+--------+
                           4   I     2  I     3  I     3  I     4  I     3  I
  Accounting                   I   6.7  I  10.0  I  10.0  I  13.3  I  10.0  I
                               +--------+--------+--------+--------+--------+
                           6   I     1  I     1  I     1  I     0  I     1  I
  Management                   I  11.1  I  11.1  I  11.1  I    .0  I  11.1  I
                               +--------+--------+--------+--------+--------+
                           7   I     2  I     2  I     1  I     0  I     1  I
  Other                        I  12.5  I  12.5  I   6.3  I    .0  I   6.3  I
                               +--------+--------+--------+--------+--------+
```

Table 93

*** CROSSTABULATION ***
INDEPENDENT VARIABLE: Prior Systems or Audit Training
by $SRMGT (group) Senior Management Involvement

```
                       Count   INot Imp Somewhat Important Extremely Imp
INDEPENDENT VARIABLE:          +--------+--------+--------+--------+
                           2   I     1  I     6  I    19  I    17  I    43
  Some                         I   2.3  I  14.0  I  44.2  I  39.5  I  44.3
                               +--------+--------+--------+--------+
                           3   I     2  I    11  I    17  I    24  I    54
  None                         I   3.7  I  20.4  I  31.5  I  44.4  I  55.7
                               +--------+--------+--------+--------+
                      Column         3       17       36       41       97
                       Total       3.1     17.5     37.1     42.3    100.0
```

Table 94

***** CROSSTABULATION *****
INDEPENDENT VARIABLE: Prior Systems or Audit Training
by $ISKEY (tabulating 1) Key Issues

```
                   Count   IInternet Intranet Virus    Access   Firewalls
                 Row pct   ISecurity Security          Controls
INDEPENDENT VARIABLE:      +--------+--------+--------+--------+--------+
                       2   I     6  I     5  I     6  I     5  I     5  I
      Some                 I  17.6  I  14.7  I  17.6  I  14.7  I  14.7  I
                           +--------+--------+--------+--------+--------+
                       3   I    10  I    13  I     9  I     4  I     4  I
      None                 I  20.8  I  27.1  I  18.8  I   8.3  I   8.3  I
                           +--------+--------+--------+--------+--------+
                  Column        16       18       15        9        9
                   Total      19.5     22.0     18.3     11.0     11.0
```

Table 94 continued

***** CROSSTABULATION *****
INDEPENDENT VARIABLE: Prior Systems or Audit Training
by $ISKEY (tabulating 1) Key Issues

```
                   Count   ICommunic Biometri Computer Other
                 Row pct   I                  Forensic Security  Row
INDEPENDENT VARIABLE:      +--------+--------+--------+--------+
                       2   I     2  I     3  I     2  I     0  I    34
      Some                 I   5.9  I   8.8  I   5.9  I    .0  I  41.5
                           +--------+--------+--------+--------+
                       3   I     4  I     1  I     2  I     1  I    48
      None                 I   8.3  I   2.1  I   4.2  I   2.1  I  58.5
                           +--------+--------+--------+--------+
                  Column         6        4        4        1       82
                   Total       7.3      4.9      4.9      1.2    100.0
```

Table 95

*** CROSSTABULATION ***
INDEPENDENT VARIABLE: Prior Systems or Audit Training by $BUSSEC (tabulating 1) Key Issues Business Security

```
                    Count  IDisaster Ecommerce Industri Info     Remote
                                               Espion   Secure   Access
                           +--------+--------+--------+--------+--------+
                        2  I     5  I     4  I     5  I     7  I     2  I
    Some                   I  15.2  I  12.1  I  15.2  I  21.2  I   6.1  I
                           +--------+--------+--------+--------+--------+
                        3  I    12  I    11  I     6  I    11  I     7  I
    None                   I  15.8  I  14.5  I   7.9  I  14.5  I   9.2  I
                           +--------+--------+--------+--------+--------+
                   Column       17       15       11       18        9
                    Total     15.6     13.8     10.1     16.5      8.3
```

Table 95 continued

*** CROSSTABULATION ***
INDEPENDENT VARIABLE: Prior Systems or Audit Training by $BUSSEC (tabulating 1) Key Issues Business Security

```
                    Count  ISecurity Software Training Year 2000
INDEPENDENT VARIABLE:      +--------+--------+--------+--------+
                        2  I     3  I     0  I     2  I     5  I     33
    Some                   I   9.1  I    .0  I   6.1  I  15.2  I   30.3
                           +--------+--------+--------+--------+
                        3  I     7  I     2  I     9  I    11  I     76
    None                   I   9.2  I   2.6  I  11.8  I  14.5  I   69.7
                           +--------+--------+--------+--------+
                   Column       10        2       11       16      109
                    Total      9.2      1.8     10.1     14.7    100.0
```

Table 96

***** CROSSTABULATION *****
INDEPENDENT VARIABLE: Prior Systems or Audit Training
by $CORPPOL (tabulating 1) Formal Security Policy

```
                  Count  ICentral  Data     External Electron Incident
                Row pct  ISecu     Class    Access   Commerce Respons
INDEPENDENT VARIABLE:    +--------+--------+--------+--------+--------+
                      2  I     6  I     4  I     6  I     3  I     8  I
   Some                  I  13.6  I   9.1  I  13.6  I   6.8  I  18.2  I
                         +--------+--------+--------+--------+--------+
                      3  I    12  I    11  I    10  I     8  I    10  I
   None                  I  11.8  I  10.8  I   9.8  I   7.8  I   9.8  I
                         +--------+--------+--------+--------+--------+
                 Column       18       15       16       11       18
                  Total     12.3     10.3     11.0      7.5     12.3
```

Table 96 continued

***** CROSSTABULATION *****
INDEPENDENT VARIABLE: Prior Systems or Audit Training
by $CORPPOL (tabulating 1) Formal Security Policy

```
                  Count  IPersonne Records  Surveill Organiza End user
                Row pct  Isecuri   Manage   ance     tion     computing
                 --------+--------+--------+--------+--------+--------+
                      2  I     5  I     5  I     3  I     0  I     4  I
   Some                  I  11.4  I  11.4  I   6.8  I    .0  I   9.1  I
                         +--------+--------+--------+--------+--------+
                      3  I    10  I    12  I    12  I     5  I    12  I
   None                  I   9.8  I  11.8  I  11.8  I   4.9  I  11.8  I
                         +--------+--------+--------+--------+--------+
                 Column       15       17       15        5       16
                  Total     10.3     11.6     10.3      3.4     11.0
```

Table 97

*** CROSSTABULATION ***
INDEPENDENT VARIABLE: Graduate Program
by $SRMGT (group) Senior Management Involvement

```
                   Count  I Not Imp Somewhat Important Extremely
INDEPENDENT VARIABLE:     +--------+--------+--------+--------+
                       1  I     1  I     4  I     4  I     7  I    16
  MBA                     I   6.3  I  25.0  I  25.0  I  43.8  I  16.5
                          +--------+--------+--------+--------+
                       2  I     0  I     1  I     2  I     1  I     4
  Ph.D                    I    .0  I  25.0  I  50.0  I  25.0  I   4.1
                          +--------+--------+--------+--------+
                       3  I     2  I     9  I    27  I    29  I    67
  MPA                     I   3.0  I  13.4  I  40.3  I  43.3  I  69.1
                          +--------+--------+--------+--------+
                       4  I     0  I     3  I     3  I     4  I    10
  PPA                     I    .0  I  30.0  I  30.0  I  40.0  I  10.3
                          +--------+--------+--------+--------+
                  Column        3       17       36       41       97
                   Total      3.1     17.5     37.1     42.3    100.0
```

Table 98

*** CROSSTABULATION ***
INDEPENDENT VARIABLE: Graduate Program
by $ISKEY (tabulating 1) Key Issues

```
                   Count  IInternet Intranet Virus    Access   Firewall
                 Row pct  ISecurit  Security          Control
INDEPENDENT VARIABLE:     +--------+--------+--------+--------+--------+
                       1  I     4  I     5  I     3  I     3  I     2  I
  MBA                     I  19.0  I  23.8  I  14.3  I  14.3  I   9.5  I
                          +--------+--------+--------+--------+--------+
                       2  I     0  I     1  I     1  I     0  I     0  I
  Ph.D                    I    .0  I  25.0  I  25.0  I    .0  I    .0  I
                          +--------+--------+--------+--------+--------+
                       3  I    11  I     9  I     9  I     5  I     6  I
  MPA                     I  22.4  I  18.4  I  18.4  I  10.2  I  12.2  I
                          +--------+--------+--------+--------+--------+
                       4  I     1  I     3  I     2  I     1  I     1  I
  PPA                     I  12.5  I  37.5  I  25.0  I  12.5  I  12.5  I
                          +--------+--------+--------+--------+--------+
                  Column       16       18       15        9        9
                   Total     19.5     22.0     18.3     11.0     11.0
```

Table 98 continued

*** CROSSTABULATION ***
INDEPENDENT VARIABLE: Graduate Program
by SISKEY (tabulating 1) Key Issues

```
                  Count   ICommunic  Biometri  Computer  Other
                 Row pct             ForensicsSecurity               Row
INDEPENDENT VARIABLE:     +---------+---------+---------+---------+
                      1   I      2  I      0  I      1  I      1  I    21
  MBA                     I    9.5  I     .0  I    4.8  I    4.8  I  25.6
                          +---------+---------+---------+---------+
                      2   I      1  I      1  I      0  I      0  I     4
  Ph.D                    I   25.0  I   25.0  I     .0  I     .0  I   4.9
                          +---------+---------+---------+---------+
                      3   I      3  I      3  I      3  I      0  I    49
  MPA                     I    6.1  I    6.1  I    6.1  I     .0  I  59.8
                          +---------+---------+---------+---------+
                      4   I      0  I      0  I      0  I      0  I     8
  PPA                     I     .0  I     .0  I     .0  I     .0  I   9.8
                          +---------+---------+---------+---------+
                 Column           6         4         4         1       82
                  Total         7.3       4.9       4.9       1.2    100.0
```

Table 99

*** * * CROSSTABULATION * * ***
INDEPENDENT VARIABLE: Graduate Program
by $BUSSEC (tabulating 1) Key Issues Business Security

```
                  Count  IDisaster Ecommerce Industri Info on  Remote
                Row pct  IRecover            Espio    Secuity  Access
INDEPENDENT VARIABLE:    +--------+--------+--------+--------+--------+
                      1  I      3 I      5 I      1 I      5 I      3 I
  MBA                    I  11.1  I  18.5  I   3.7  I  18.5  I  11.1  I
                         +--------+--------+--------+--------+--------+
                      2  I      1 I      0 I      0 I      0 I      1 I
  Ph.D                   I  33.3  I    .0  I    .0  I    .0  I  33.3  I
                         +--------+--------+--------+--------+--------+
                      3  I     11 I      8 I      8 I     12 I      3 I
  MPA                    I  16.2  I  11.8  I  11.8  I  17.6  I   4.4  I
                         +--------+--------+--------+--------+--------+
                      4  I      2 I      2 I      2 I      1 I      2 I
  PPA                    I  18.2  I  18.2  I  18.2  I   9.1  I  18.2  I
                         +--------+--------+--------+--------+--------+
                 Column        17       15       11       18        9
                  Total      15.6     13.8     10.1     16.5      8.3
```

Table 99 continued

*** * * CROSSTABULATION * * ***
INDEPENDENT VARIABLE: Graduate Program
by $BUSSEC (tabulating 1) Key Issues Business Security

```
                  Count  ISecurity Software Training Year 2000
INDEPENDENT VARIABLE:    +--------+--------+--------+--------+
                      1  I      2 I      0 I      4 I      4 I     27
  MBA                    I   7.4  I    .0  I  14.8  I  14.8  I   24.8
                         +--------+--------+--------+--------+
                      2  I      0 I      0 I      1 I      0 I      3
  Ph.D                   I    .0  I    .0  I  33.3  I    .0  I    2.8
                         +--------+--------+--------+--------+
                      3  I      8 I      2 I      6 I     10 I     68
  MPA                    I  11.8  I   2.9  I   8.8  I  14.7  I   62.4
                         +--------+--------+--------+--------+
                      4  I      0 I      0 I      0 I      2 I     11
  PPA                    I    .0  I    .0  I    .0  I  18.2  I   10.1
                         +--------+--------+--------+--------+
                 Column        10        2       11       16      109
                  Total       9.2      1.8     10.1     14.7    100.0
```

Table 100

*** CROSSTABULATION ***
INDEPENDENT VARIABLE: Graduate Program
by $CORPPOL (tabulating 1) Formal Security Policy

```
                    Count  Icentral  Data cla External Electron Incident
                  Row pct  ISecu     Class    Access   Commerce  Response
INDEPENDENT VARIABLE:      +--------+--------+--------+--------+--------+
                        1  I     4  I     5  I     5  I     4  I     4  I
  MBA                      I   9.1  I  11.4  I  11.4  I   9.1  I   9.1  I
                           +--------+--------+--------+--------+--------+
                        2  I     1  I     1  I     1  I     1  I     1  I
  Ph.D                     I  11.1  I  11.1  I  11.1  I  11.1  I  11.1  I
                           +--------+--------+--------+--------+--------+
                        3  I    11  I     8  I     9  I     4  I    11  I
  MPA                      I  13.8  I  10.0  I  11.3  I   5.0  I  13.8  I
                           +--------+--------+--------+--------+--------+
                        4  I     2  I     1  I     1  I     2  I     2  I
  PPA                      I  15.4  I   7.7  I   7.7  I  15.4  I  15.4  I
                           +--------+--------+--------+--------+--------+
                   Column       18       15       16       11       18
                    Total     12.3     10.3     11.0      7.5     12.3
```

Table 100 continued

*** * * CROSSTABULATION * * ***
INDEPENDENT VARIABLE: Graduate Program
by $CORPPOL (tabulating 1) Formal Security Policy

```
                      Count  IPersonne Records  Surveill Organiza End user
INDEPENDENT VARIABLE: -+--------+--------+--------+--------+--------+
                         1 I      4 I      5 I      5 I      3 I      5 I
  MBA                      I    9.1 I   11.4 I   11.4 I    6.8 I   11.4 I
                           +--------+--------+--------+--------+--------+
                         2 I      1 I      1 I      1 I      0 I      1 I
  Ph.D                     I   11.1 I   11.1 I   11.1 I     .0 I   11.1 I
                           +--------+--------+--------+--------+--------+
                         3 I      9 I     10 I      8 I      1 I      9 I
  MPA                      I   11.3 I   12.5 I   10.0 I    1.3 I   11.3 I
                           +--------+--------+--------+--------+--------+
                         4 I      1 I      1 I      1 I      1 I      1 I
  PPA                      I    7.7 I    7.7 I    7.7 I    7.7 I    7.7 I
                           +--------+--------+--------+--------+--------+
                     Column      15       17       15        5       16
                      Total    10.3     11.6     10.3      3.4     11.0
```

Table 101

*** * * CROSSTABULATION * * ***
INDEPENDENT VARIABLE: Undergraduate Education
by $SRMGT (group) Senior Management Involvement

```
                      Count  INot Imp Somewhat Important Extreme
                    Row pct  I         Important         Important  Row
INDEPENDENT VARIABLE:        +--------+--------+--------+--------+
                          1  I      0 I      3 I      1 I      7 I    11
  Liberal Arts               I     .0 I   27.3 I    9.1 I   63.6 I   11.3
                             +--------+--------+--------+--------+
                          2  I      1 I      7 I     25 I     22 I    55
  Business                   I    1.8 I   12.7 I   45.5 I   40.0 I   56.7
                             +--------+--------+--------+--------+
                          3  I      2 I      7 I     10 I     12 I    31
  Engineering/Sciences       I    6.5 I   22.6 I   32.3 I   38.7 I   32.0
                             +--------+--------+--------+--------+
                     Column         3       17       36       41      97
                      Total       3.1     17.5     37.1     42.3   100.0
```

Table 102

*** CROSSTABULATION ***
INDEPENDENT VARIABLE: Undergraduate Education
by $ISKEY (tabulating 1) Key Issues

	Count Row pct	Internet Security	Intranet Security	Virus	Access Control	Firewalls
	1	3	4	3	1	1
Liberal Arts		23.1	30.8	23.1	7.7	7.7
	2	9	9	8	6	5
Business		19.6	19.6	17.4	13.0	10.9
	3	4	5	4	2	3
Engineering/Sciences		17.4	21.7	17.4	8.7	13.0
	Column	16	18	15	9	9
	Total	19.5	22.0	18.3	11.0	11.0

Table 103

*** CROSSTABULATION ***
INDEPENDENT VARIABLE: Undergraduate Education
by $ISKEY (tabulating 1) Key Issues

	Count Row pct	Communic	Biometric	Computer Forensic	Other Security	Row
INDEPENDENT VARIABLE:						
	1	0	1	0	0	13
Liberal Arts		.0	7.7	.0	.0	15.9
	2	3	1	4	1	46
Business		6.5	2.2	8.7	2.2	56.1
	3	3	2	0	0	23
Engineering/Sciences		13.0	8.7	.0	.0	28.0
	Column	6	4	4	1	82
	Total	7.3	4.9	4.9	1.2	100.0

Table 104

*** CROSSTABULATION ***

INDEPENDENT VARIABLE: Undergraduate Education
by $BUSSEC (tabulating 1) Key Issues Business Security

```
                       Count  IDisaster E commer Industri Info on  Remote A
                     Row pct  IRecover           Espio    Key Secu Access
                              +--------+--------+--------+--------+--------+
                           1  I     3  I     3  I     2  I     3  I     1  I
  Liberal Arts                I  17.6  I  17.6  I  11.8  I  17.6  I   5.9  I
                              +--------+--------+--------+--------+--------+
                           2  I    10  I     8  I     6  I    11  I     3  I
    Business                  I  16.1  I  12.9  I   9.7  I  17.7  I   4.8  I
                              +--------+--------+--------+--------+--------+
                           3  I     4  I     4  I     3  I     4  I     5  I
    Engineering/Sciences      I  13.3  I  13.3  I  10.0  I  13.3  I  16.7  I
                              +--------+--------+--------+--------+--------+
                      Column       17       15       11       18        9
                       Total     15.6     13.8     10.1     16.5      8.3    0
```

Table 105

*** CROSSTABULATION ***

INDEPENDENT VARIABLE: Undergraduate Education
by $BUSSEC (tabulating 1) Key Issues Business Security

```
                       Count  ISecurity Software Training Year 2000
                     --------+--------+--------+--------+--------+
                           1  I     0  I     0  I     2  I     3  I    17
    Liberal Arts              I    .0  I    .0  I  11.8  I  17.6  I  15.6
                              +--------+--------+--------+--------+
                           2  I     8  I     1  I     5  I    10  I    62
    Business                  I  12.9  I   1.6  I   8.1  I  16.1  I  56.9
                              +--------+--------+--------+--------+
                           3  I     2  I     1  I     4  I     3  I    30
    Engineering/Sciences      I   6.7  I   3.3  I  13.3  I  10.0  I  27.5
                              +--------+--------+--------+--------+
                      Column       10        2       11       16      109
                       Total      9.2      1.8     10.1     14.7    100.0
```

Table 106

*** CROSSTABULATION ***
INDEPENDENT VARIABLE: Undergraduate Education
by $CORPPOL (tabulating 1) Formal Security Policy

```
                   Count   ICentrali Data     External Electron Incident
                 Row pct   I Sec     Class    Access   Commerce Respons
INDEPENDENT VARIABLE:      +--------+--------+--------+--------+--------+
                       1   I     3  I     3  I     3  I     1  I     2  I
Liberal Arts               I  13.0  I  13.0  I  13.0  I   4.3  I   8.7  I
                           +--------+--------+--------+--------+--------+
                       2   I     9  I     6  I     7  I     4  I     9  I
  Business                 I  13.6  I   9.1  I  10.6  I   6.1  I  13.6  I
                           +--------+--------+--------+--------+--------+
                       3   I     6  I     6  I     6  I     6  I     7  I
  Engineering/Sciences     I  10.5  I  10.5  I  10.5  I  10.5  I  12.3  I
                           +--------+--------+--------+--------+--------+
                  Column        18       15       16       11       18
                   Total      12.3     10.3     11.0      7.5     12.3
```

Table 107

*** CROSSTABULATION ***
INDEPENDENT VARIABLE: Undergraduate Education
by $CORPPOL (tabulating 1) Formal Security Policy

```
                   Count   IPersonne Records  Surveill Organiza End user
                 Row pct   Isecuri   Manage                     Computing
INDEPENDENT VARIABLE:      +--------+--------+--------+--------+--------+
                       1   I     2  I     3  I     2  I     2  I     2  I
  Liberal Arts             I   8.7  I  13.0  I   8.7  I   8.7  I   8.7  I
                           +--------+--------+--------+--------+--------+
                       2   I     7  I     8  I     7  I     1  I     8  I
  Business                 I  10.6  I  12.1  I  10.6  I   1.5  I  12.1  I
                           +--------+--------+--------+--------+--------+
                       3   I     6  I     6  I     6  I     2  I     6  I
  Engineering/Sciences     I  10.5  I  10.5  I  10.5  I   3.5  I  10.5  I
                           +--------+--------+--------+--------+--------+
                  Column        15       17       15        5       16
                   Total      10.3     11.6     10.3      3.4     11.0
```

Table 108

*** C R O S S T A B U L A T I O N ***
INDEPENDENT VARIABLE: Work Experience
by $SRMGT (group) Senior Management Involvement

```
                       Count  INot Imp Somewhat Important Extremely
                     Row pct  I        Important          Imporant  Row
                              I     1  I     2  I     3  I     4  I
INDEPENDENT VARIABLE:         +--------+--------+--------+--------+
                           1  I     2  I     9  I    14  I    20  I    45
  None                        I   4.4  I  20.0  I  31.1  I  44.4  I  46.4
                              +--------+--------+--------+--------+
                           2  I     0  I     1  I     9  I     8  I    18
  1- 2 years                  I    .0  I   5.6  I  50.0  I  44.4  I  18.6
                              +--------+--------+--------+--------+
                           3  I     1  I     2  I     9  I     3  I    15
  3 - 5 years                 I   6.7  I  13.3  I  60.0  I  20.0  I  15.5
                              +--------+--------+--------+--------+
                           4  I     0  I     0  I     0  I     1  I     1
  5 - 10 years                I    .0  I    .0  I    .0  I 100.0  I   1.0
                              +--------+--------+--------+--------+
                           5  I     0  I     5  I     4  I     9  I    18
  10+ years                   I    .0  I  27.8  I  22.2  I  50.0  I  18.6
                              +--------+--------+--------+--------+
                      Column        3       17       36       41       97
                       Total      3.1     17.5     37.1     42.3    100.0
```

Table 109
*** CROSSTABULATION ***
INDEPENDENT VARIABLE: Work Experience
by $ISKEY (tabulating 1) Key Issues

```
                          Count   IInternet Intranet Virus    Access   Firewalls
                          Row pctISecurity Security           Control
                                  +--------+--------+--------+--------+--------+
                                1 I      7 I      6 I      6 I      3 I      3 I
None                              I   24.1 I   20.7 I   20.7 I   10.3 I   10.3 I
                                  +--------+--------+--------+--------+--------+
                                2 I      3 I      3 I      1 I      2 I      2 I
  1- 2 years                      I   20.0 I   20.0 I    6.7 I   13.3 I   13.3 I
                                  +--------+--------+--------+--------+--------+
                                3 I      2 I      2 I      1 I      1 I      0 I
  3 - 5 years                     I   33.3 I   33.3 I   16.7 I   16.7 I     .0 I
                                  +--------+--------+--------+--------+--------+
                                4 I      1 I      1 I      1 I      0 I      0 I
  5 - 10 years                    I   33.3 I   33.3 I   33.3 I     .0 I     .0 I
                                  +--------+--------+--------+--------+--------+
                                5 I      3 I      6 I      6 I      3 I      4 I
  10+ years                       I   10.3 I   20.7 I   20.7 I   10.3 I   13.8 I
                                  +--------+--------+--------+--------+--------+
                          Total       19.5     22.0     18.3     11.0     11.0
```

Table 109 continued

*** CROSSTABULATION ***
INDEPENDENT VARIABLE: Work Experience
by $ISKEY (tabulating 1) Key Issues

```
                  Count   ICommunic Biometrics Computer Other
                Row pct I                     Forensics Security Row

INDEPENDENT VARIABLE:   +--------+--------+--------+--------+
                      1 I      1 I      0 I      3 I      0 I    29
  None                  I    3.4 I     .0 I   10.3 I     .0 I  35.4
                        +--------+--------+--------+--------+
                      2 I      2 I      2 I      0 I      0 I    15
  1- 2 years            I   13.3 I   13.3 I     .0 I     .0 I  18.3
                        +--------+--------+--------+--------+
                      3 I      0 I      0 I      0 I      0 I     6
  3 - 5 years           I     .0 I     .0 I     .0 I     .0 I   7.3
                        +--------+--------+--------+--------+
                      4 I      0 I      0 I      0 I      0 I     3
  5 - 10 years          I     .0 I     .0 I     .0 I     .0 I   3.7
                        +--------+--------+--------+--------+
                      5 I      3 I      2 I      1 I      1 I    29
  10+ years             I   10.3 I    6.9 I    3.4 I    3.4 I  35.4
                        +--------+--------+--------+--------+
                 Column        6        4        4        1     82
                  Total      7.3      4.9      4.9      1.2  100.0
```

Table 110

*** CROSSTABULATION ***
INDEPENDENT VARIABLE: Work Experience
by $BUSSEC (tabulating 1) Key Issues Business Security

```
                            Count   IDisaster Ecommerce Industri Info     Remote
                            Row pct IRecovery           Espionage Secu    Access
                            --------+--------+--------+--------+--------+--------+
                                  1 I      7 I      6 I      3 I      8 I      2 I
   None                             I   16.3 I   14.0 I    7.0 I   18.6 I    4.7 I
                                    +--------+--------+--------+--------+--------+
                                  2 I      1 I      3 I      4 I      4 I      1 I
 1- 2 years                         I    5.6 I   16.7 I   22.2 I   22.2 I    5.6 I
                                    +--------+--------+--------+--------+--------+
                                  3 I      2 I      2 I      0 I      2 I      1 I
   3 - 5 years                      I   14.3 I   14.3 I     .0 I   14.3 I    7.1 I
                                    +--------+--------+--------+--------+--------+
                                  4 I      1 I      1 I      0 I      1 I      0 I
   5 - 10 years                     I   33.3 I   33.3 I     .0 I   33.3 I     .0 I
                                    +--------+--------+--------+--------+--------+
                                  5 I      6 I      3 I      4 I      3 I      5 I
   10+ years                        I   19.4 I    9.7 I   12.9 I    9.7 I   16.1 I
                                    +--------+--------+--------+--------+--------+
                            Column        17       15       11       18        9
                             Total      15.6     13.8     10.1     16.5      8.3
```

Table 110 continued

***** CROSSTABULATION *****
INDEPENDENT VARIABLE: Work Experience
by $BUSSEC (tabulating 1) Key Issues Business Security

```
                          Count  ISecurity Software Training Year 2000
INDEPENDENT VARIABLE:            +--------+--------+--------+--------+
                              1  I     6  I     1  I     5  I     5  I    43
    None                         I  14.0  I   2.3  I  11.6  I  11.6  I  39.4
                                 +--------+--------+--------+--------+
                              2  I     1  I     0  I     0  I     4  I    18
    1- 2 years                   I   5.6  I    .0  I    .0  I  22.2  I  16.5
                                 +--------+--------+--------+--------+
                              3  I     1  I     1  I     2  I     3  I    14
    3 - 5 years                  I   7.1  I   7.1  I  14.3  I  21.4  I  12.8
                                 +--------+--------+--------+--------+
                              4  I     0  I     0  I     0  I     0  I     3
    5 - 10 years                 I    .0  I    .0  I    .0  I    .0  I   2.8
                                 +--------+--------+--------+--------+
                              5  I     2  I     0  I     4  I     4  I    31
    10+ years                    I   6.5  I    .0  I  12.9  I  12.9  I  28.4
                                 +--------+--------+--------+--------+
                         Column       10        2       11       16      109
                          Total      9.2      1.8     10.1     14.7    100.0
```

Table 111

*** * * CROSSTABULATION * * ***
INDEPENDENT VARIABLE: Work Experience
by $CORPPOL (tabulating 1) Formal Security Policy

```
                    Count  ICentrali Data     External Electron Incident
                  Row pct  I         Class    Access   Commerce Response
INDEPENDENT VARIABLE:      +--------+--------+--------+--------+--------+
                        1  I      6 I      4 I      5 I      1 I      6 I
  None                     I   13.6 I    9.1 I   11.4 I    2.3 I   13.6 I
                           +--------+--------+--------+--------+--------+
                        2  I      3 I      3 I      3 I      3 I      4 I
  1- 2 years               I   10.3 I   10.3 I   10.3 I   10.3 I   13.8 I
                           +--------+--------+--------+--------+--------+
                           I      2 I      2 I      2 I      2 I      2 I
  3 - 5 years              I   10.5 I   10.5 I   10.5 I   10.5 I   10.5 I
                           +--------+--------+--------+--------+--------+
                           I      1 I      1 I      1 I      1 I      1 I
  5 - 10 years             I   11.1 I   11.1 I   11.1 I   11.1 I   11.1 I
                           +--------+--------+--------+--------+--------+
                           I      6 I      5 I      5 I      4 I      5
      10+ years            I   13.3 I   11.1 I   11.1 I    8.9 I   11.1 I
                           +--------+--------+--------+--------+--------+
                   Column        18       15       16       11       18
                    Total      12.3     10.3     11.0      7.5     12.3
```

Table 111 continued

INDEPENDENT VARIABLE: Work Experience
by $CORPPOL (tabulating 1) Formal Security Policy

```
                    Count  IPersonne Records  Surveill Organiza End user
                  Row pct  ISecurity Manageme                   Computing
INDEPENDENT VARIABLE:      +--------+--------+--------+--------+--------+
                        1  I     3  I     6  I     5  I     2  I     6  I
None                       I   6.8  I  13.6  I  11.4  I   4.5  I  13.6  I
                           +--------+--------+--------+--------+--------+
                        2  I     4  I     3  I     3  I     0  I     3  I
1- 2 years                 I  13.8  I  10.3  I  10.3  I    .0  I  10.3  I
                           +--------+--------+--------+--------+--------+
                        3  I     2  I     2  I     2  I     1  I     2  I
3 - 5 years                I  10.5  I  10.5  I  10.5  I   5.3  I  10.5  I
                           +--------+--------+--------+--------+--------+
                        4  I     1  I     1  I     1  I     0  I     1  I
5 - 10 years               I  11.1  I  11.1  I  11.1  I    .0  I  11.1  I
                           +--------+--------+--------+--------+--------+
                        5  I     5  I     5  I     4  I     2  I     4  I
  10+ years                I  11.1  I  11.1  I   8.9  I   4.4  I   8.9  I
                           +--------+--------+--------+--------+--------+
                   Column       15       17       15        5       16
                    Total     10.3     11.6     10.3      3.4     11.0
```

APPENDIX E: STATISTICAL SOFTWARE TOOLS

SPSS for Windows, Release 7.5 was used for data tabulation, descriptive statistics, and data exploration. *SPSS* was employed for hypothesis testing using the ANOVA and multiple response cross tabulation tests for association between security issues and the six independent variables.

SPSS was used to generate frequency tables, crosstabulation tables and ANOVA tables.

APPENDIX F: TECHNICAL SYSTEMS INFORMATION

Text for the proposal and dissertation was processed using *MS Word 95.*

Bibliographic Control was provided through the use of *EndNote, Windows Version 3.0.*

Text was processed on an *IBM ThinkPad 380D*, running *Windows 95.*

Text was printed on a *Hewlett Packarf Laserjet*I with *Postscript Times Roman Font.*

BIBLIOGRAPHY

Agarwal, R., Prayesh, J. (1995). A Field Study of the Role of Innovation Characteristiccs in the Information Technology Adoption Process. *University of Dayton Working Paper.*

Agarwal, R., Tanniru, M. Wilemon, D. (1995). Assimilating Information Technology Innovations: Strategies and Moderating Influences. *University of Dayton Working Paper.*

Ajzen, I., Fisbein, M. (1980). *Understanding Attitudes and Predicting Behavior.* Englewood Cliffs, NJ: Prentice-Hall.

Alexander, M. (1995). Make It A Policy To Protect Yourself. *Datamation, December 1, 1995*(41:22), 59.

Anonymous (1997). *Maximum Security: A Hacker's Guide to Protecting Your Internet Site and Network.* Indianapolis: sams.net.

Applegate, L. M. (1994). Managing in an Information Age: Transforming the Organization of the 1990s. In S. S. R. Baskerville, O. Ngwenyaman, J. DeGross (Ed.), *Transforming Organizations with Information Technology* (pp. 15-94). Amsterdam: North-Holland.

Artz, J. M. (1994). *Virtue vs. Utility: Alternative Foundations for Computer Ethics.* Paper presented at the Ethics in the Computer Age, Gatlinburg, TN USA.

Athey, T. H., and Zmud, R.W. (1988). *Introduction to Computers and Information Systems.* (2nd Edition ed.). Glenville, IL: Scott, Foresman and Company.

Attewell, P. (1992). Technology Diffusion and Organizational Learning: The Case of Business Computing. *Organizational Science, 3 (1)*, 1-19.

Babbie, E. (1992). *The Practice of Social Science Research.* (6th edition ed.). Belmont, CA: Wadsworth Publishing.

Ball, L., and Harris, R. (1982). SMIS Member: A Membership Analysis. *MIS Quarterly, March 1982*(6:1), 19-38.

Barrett, E. (1989). Sensemaking, Learning, and the Online Environment. In E. Barrett (Ed.), *The Society of Text.* Cambridge, MA: MIT Press.

Baskerville, R. (1991). Risk Analysis: An Interpretive Feasibility Tool in Justifying Information Systems Security. *European Journal of Information Systems* (1:2), 121-130.

Baskerville, R. (1993). Information Systems Security Design Methods: Implications for Information Systems Development. *ACM Computing Surveys, December 1993*(25:4), 375-414.

Benjamin, R. J., Blunt, J. (1992). Critical IT Issues: The Next 10 Years. *Sloan Management Review, 33 (4)*(Summer), 7-19.

Bice, M. O. (1990). CEO Commitment Key to Organizational Change. *Hospitals, 62 (2)*(January 1990), 76.

Bicknell, D. (1995). How to Avoid Getting Snared by the Net. *Computer Weekly, November 16, 1995*, 20.

Bijker, W., Brancheau, J., and Ramiller, N. (1995). *Innovation - the Very Idea: Exploring Terms of Research on IS/IT Innovations*. Paper presented at the 16th International Conference on Information Systems, Amsterdam.

Bishop, M., and Klein, D. (1995). Improving System Security via Proactive Password Checking. *Computers and Security* (14:3), 233-249.

Boone, M. (1991). *Leadership and the Computer*. Rocklin, CA: Prima Publishing.

Bostrom, R. P., and Heinen, J.S. (1977). MIS Problems and Failures: A Socio-technical Perspective, Part I - The Causes. *MIS Quarterly, 1 (3)*, 17-32.

Brancheau, J. C., and Wetherbe, J.C. (1987). Key Issues in Information Systems Management. *MIS Quarterly, March 1987*(12:2), 23-36.

Brancheau, J. C., Wetherbe, J.C. (1990). The Adoption of Spreadsheet Software: Testing Innovation Diffusion Theory in the Context of End-User Computing. *Information Systems Research, 1(1)*, 41-64.

Brancheau, J. C., Wetherbe, J.C. (1991). The Adoption of Spreadsheet Software: Testing Innovation Diffusion Theory in the Context of End-User Computing. *Information Systems Research, 1 (2)*, 115-143.

Brand, S., and Makey, J. (1985). *Department of Defense Password Management Guideline* (CSC-STD-002-85). Department of Defense.

Burns, T., and Stalker, G.M. (1961). *The Management of Innovation.* London: Tavistock.

Calder, B., and Schurr, P. (1981). Attitudinal Processes in Organizations. *Research Organizational Behavior, 3,* 283-302.

Carter, R. (1988). Dependence and Disaster: Recovering From EDP Systems Failure. *Management Services (UK), December 1988*(32:12), 20-22.

Cheney, P. H., Dickson, G.W. (1982). Organizational Characteristics and Information Systems: An Exploratory Investigation. *Academy of Management Journal, 25(1)*(March 1982), 170-184.

Cheswick, W.R. (1991). "An Evening with Berferd, in Which a Cracker is Lured, Endured, and Studied." Available via ftp from research.att.com.

Chorafas, D. and Steinmann, H. (1990). *Intelligent Networks.* Boca Raton, FL: Multiscience Press.

Clark, D., and Wilson, D. (1987). *A Comparison of Commercial and Military Computer Security Policies.* Paper presented at the Proceeding of the IEEE Symposium on Security and Privacy, New York.

Cleveland, H. (1985). *The Knowledge Executive: Leadership in an Information Society.* New York: Truman Talley.

Cohen, W. M. and Levinthal, D.A. (1990). Absorptive Capacity: A New Perspective on Learning and Innovation. *Administrative Science Quarterly, 35,* 123-139.

Computer Security Institute. (1998). *Computer Crime and Security Survey* . Computer Security Institute.

Computer Security Institute. (1998). *Issues and Trends: 1998 CSI/FBI Computer Crime and Security Survey* . Computer Security Institute.

Conger, S., and Loch, Karen D. (1995). Ethics and Computer Use. *Communications of the ACM, December 1995*(38:12), 30-32.

Cooper, R. B., Zmud, R.W. (1990). Information Technology Implementation Research: A Technological Diffusion Approach. *Management Science, 36 (2),* 123-139.

Couger, J. D. (1989). Preparing IS Students to Deal with Ethical Issues. *MIS Quarterly, June 1989*(12:2).

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly, 13(3)*(September 1989), 319-339.

Davis, F. D., Bagozzi, R.P., Warshaw, P.R. (1989). User Acceptance of Computer Technology: A Comparison of Two Theoretical Models. *Management Science, 35 (8)*, 982-1003.

Davis, F. G. F., Gantenbein, R.E. (1987). Recovering from a Computer Virus Attack. *Journal of Systems and Software, December 1987*(7:4), 253-258.

DeLisi, P. S. (1990). Lessons from the Steel Axe: Culture, Technology, and Organizational Change. *Sloan Management Review, 32 (1)*(Fall 1990), 83-93.

Demaline, R. E., & Quinn, W.D. (1979). *Hints for Planning and Conducting a Survey and Bibliography of Survey Methods.* Kalamazoo, MI: Western Michigan University Evaluation Center.

Denning, D. E., and Denning, P. J. (1998). *Internet Besieged: Countering Cyberspace Scofflaws*. Reading, Massachusetts: Addison Wesley.

Denning, D. E., and MacDoran, Peter F. (1998). Location-based Authentication: Grounding Cyberspace for Better Security. , *Internet Besieged.* Reading, Massachusetts: Addison Wesley.

Denning, P. J. (1990). *Computers Under Attack.* New York: Addison-Wesley.

Dixon, P. J., and John, D.A. (1989). Technology Issues Facing Corporate Management in the 1990s. *MIS Quarterly, September 1989*(13:3), 247-255.

Dreyfus, H. and. Dreyfus, S. (1986). *Mind Over Machine: The Power of Human Intuition and Expertise in the Era of the Computer.* New York: Free Press.

Eichin, M., and Rochlis, M. (1989). "With Microscope and Tweezers: An Analysis of the Internet Worm of 1988," available via ftp from athena.mit.edu

Ernst & Young (1997). *5th Annual Information Security Survey.* Available at http://www.ey.com/publicate/tce.

Ernst & Young. (1995). *3rd Annual Information Security Survey* . Available at http://www.ey.com/publicate/tce.

Ernst & Young. (1996). 4th Annual Information Security Survey. Available at http://www.ey.com/publicate/tce.

Farhoomand, A. F. (1989). Managing Computer Security. *Datamation, January 1, 1989*(26:34), 67.

Farmer, D. (1996). *A Semi Statistical Security Survey of Key Internet Hosts*. Available at http://www.fish.com/survey/introduction.html.

Fichman, F. D., Bagozzi, R.P., Kemerer, C.F. (1995). The Assimilation of Software Prcess Innovations: An Organizational Learning Perspective. *MIT Center for Information Systems Working Paper 281, July 1995.*

Fichman, R. G., Kemerer, C.F. (1993). Adoption of Software Engineering Process Innovations: The Cse of Object Orientation. *Sloan Management Review* (Winter 1993), 7-23.

Fichman, R. G., Kemerer, C.F. (1994). Toward A Theory of the Adoption and Diffusion of Software Process Innovations. *Proceedings of the International Federation of Information Processing, A-45*, 23-30.

Fites, P., and Kraatz, M. (1993). *Information Systems Security: A Practioner's Reference*. New York: Van Nostrand Reinhold.

Flamm, K. (1989). *Targeting the Computer*. Washington, D.C.: Brookings Institute.

Fuerst, W. L., Cheney, P.H. (1982). Factors Affecting The Perceived Utilization of Computer-Based Decision Support Systems in the Oil Industry. *Decision Sciences, 3(4)*, 554-569.

Galbraith, J. (1973). *Designing Complex Organizations*. Reading, MA: Addison-Wesley Publishing.

Gallivan, M. J. (1996). *Strategies for Implementing New Software Processes: An Evaluation of a Contingency Framework*. Paper presented at the SIGCPR/SIGMIS 1996, Denver, Colorado.

Gallivan, M. J., Hofman, J.D., Orlikowski, W.J. (1994). *Implementing Radical Change; Gradual versus Rapid Pace*. Paper presented at the 15th International Conference on Information Systems, Vancouver.

Gash, D. C., and Orlinkowski, W.J. (1991). Changing Frames: Towards an Understanding of Information Technology and Organizational Change. *Academy of Management Best Papers Proceedings, 51st Annual Meeting*, 189-193.

Gatigon, H., Robertson, T.S. (1989). Technology Diffusion: An Empirical Test of Competitive Effects. *Journal of Marketing, 52*(january 1989), 35-49.

Grief, I. (1988). *Computer-supported Cooperative Work: a Book of Readings.* San Mateo, CA: Morgan Kaufmann Publishers.

Harasim, L. (1987). *Computer-mediated Cooperation in Education: Group Learning Networks, Proceedings of the Second Symposium on Computer Conferencing.* Guelph, Ontario Canada: University of Guelph.

Harmon, G. (1993). On the Evolution of Information Science. *Journal of the American Society for Information Science, 22*, 235-241.

Harrington, S. J. (1996). The Effects of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions. *MIS Quarterly, September 1996*, 257-278.

Hartmanis J.,and Lin, H. (1992). *Computing the future: A broader agenda for computer science and engineering.* Washington, D.C.: National Academy Press.

Hartog, C., and Rouse, R. A. (1987). A Blueprint for the New IS Professional. *Datamation, 1987* (33:20), 64-69.

Hartog, C., Herbert, M. (1986). 1985 Opinion Survey of MIS Managers; Key Issues. *MIS Quarterly, December 1986*(10:4), 351-361.

Helsinki University of Technology (1998). *International Cryptography.* Available online at http://www.cs.hut.fi/ssh/crypto/.

Herbert, M., and Hartog, Curt (1986). MIS Rates the Issues. *Datamation, November 15, 1986*(32:22), 79-86.

Hiltz, S. a. T., M. (1993). *The Network Nation: Human Communication Via Computer.* (Revised edition ed.). Cambridge, MA: MIT Press.

Hinkle, D. E., Wiersma, W., and Jurs, S.G. (1988). *Applied Statistics for the Behavioral Sciences, 2nd edition.* Boston, MA.: Houghton Mifflin.

Hoffer, J., Straub, D.W. (1989). The 9 to 5 Underground: Are You Policing Computer Crimes? *Sloan Management Review, Summer 1989*, 351-361.

Hollinger, R. (1991). Hackers: Computer Heroes or Electronic Highwaymen? *Computers & Society, June 1991*(21:1), 6-17.

Howard, J. (1997). *An Analysis of Security Incidents on the Internet: 1989-1995.* Ph.D Dissertation, Carnegie Mellon University.

Huber, G. P. (1984). The Nature and Design of Postindustrial Organizations. *Management Science*(30:8), 928-951.

Huff, S. L., Munro, M.C. (1985). Information Technology Assessment and Adoption: A Field Study. *MIS Quarterly*, *9(4)*(September 1989), 319-339.

Hunsucker, J. D., Loos, D. (1989). Transition Management: An Analysis of Strategic Considerations for Effective Implementation. *Engineering Management International*, *5 (3)* (February 1989), 167-178.

Hutt, A. E., Bosworth, Seymour, and Hooyt, Douglas B. (1995). *Computer Security Handbook*. New York: John Wiley & Sons.

IEEE (1983). The Best Techniques for Computer Security. *Computer*, *January 1983*(16:7), 86.

Jajodia, S. (1996). Database Security and Privacy. *ACM Computing Surveys*, *March*(28:1), 129-131.

Katzenbach, J., & Smith, D. (1993). *The Wisdom of Teams*. Cambridge, MA: Harvard Press.

Keating, J. (1998). Internet Globalization and the Proliferation of Computer Crime. (Vol. 1998): CJ Europe Online.

Keen, P. G. W. (1981). Information Systems and Organizational Change. *Communications of the ACM*, *24 (1)*(January 1981), 24-33.

Kiesler, S. (1986). The Hidden Message in Computer Networks. *Harvard Business Review*, *64*(1), 46-48,52,54,58,60.

Kizza, J. M. (1994). *Combating Computer Crimes: A Long Term Strategy*. Paper presented at the Ethics in the Computer Age, Gatlinburg, TN USA.

Klein, D. V. Foiling the Cracker: A Survey of and Improvements to Password Security.

Kling, R. (1980). Computer Abuse and Computer Crime as Organizational Activities. *Computers and Law*, *Spring 1980*(2).

Kwon, S. L., and Zmud, R.W. (1987). Unifying the Fragmented Models of Information Systems Implementation. In R. J. Boland, Hirscheim, R.A. (Ed.), *Critical Issues in Information Systems Research* (pp. 227-251). New York: John Wiley & Sons.

Landau, S., Kent, S., Brooks, C., Charney, S., Denning, D., Diffie, W., Lauck, A., Miller, D., Neumann, P., and Sobel, D. (1994). Crypto Policy Perspectives. *Communications of the ACM, August 1994*(37:8), 115.

Landwehr, C. E. (1981). Formal Models for Computer Security. *ACM Computing Surveys, September 1981*(13:3), 247-278.

Landwehr, C., Alan R., McDermott, J. P., and Choi, W. S. (1994). A Taxonomy of Computer Program Security Flaws. *ACM Computing Surveys, September 1994*(26:3), 211-254.

Laudon, K. C. (1995). Ethical Concepts and Information Technology: Ethics and Computer Use. *Communications of the ACM, December 1995*(38:12), 33.

Lee, J. A., Segal, G. and Steier.R. (1986). A Report on the ACM Panel on Hacking. *Communications of the ACM, April 1986*(29:4), 297-299.

Lehmann, F. (1987). Computer Break Ins. *Communications of the ACM, July 1987*(30:7), 584-585.

Leibrock, L. R. (1994). *Computer-supported Collaborative Work Experiments in the Polysemy of Cognition, Education, and Learning Organizations*, The University of Texas at Austin.

Leonard-Barton, D. (1987). Implementing Structured Software Methodologies: A Case of Innovation in Process Technology. *Interfaces, 17*, 6-17.

Leonard-Barton, D. (1988). Implementation Characteristics of Organizational Innovations: Limits and Opportunities for Management Strategies. *Communications Research, 15 (5)*, 603-631.

Leonard-Barton, D., and Deschamps, I. (1988). Managerial Influence in the Implementation of New Technology. *Management Science, 14*, 1252-1265.

Leveson, N., and Turner, C.S. (1992). *An Investigation of the Therac 25 Accidents* . Information and Computer Science Department.

Lind, M. R., Zmud, R.W. (1991). The Influence of a Convergence in Understanding Between Technology Providers and Users on Information Technology Innovativeness. *Organizational Science, 2 (2)*, 195-217.

Loch, K. D., and Conger, S (1996). Evaluating Ethical Decision Making and Computer Use. *Communications of the ACM, July 1996*(39:7), 74-83.

Loch, K. D., Carr, H.H., and Warkentin, M.E. (1992). Threats to Information Systems: Today's Reality, Yesterday's Understanding. *MIS Quarterly, June 1992*(16:2), 173-186.

Lucas, H. C. J. (1975). *Why Information Systems Fail.* New York: Columbia University Press.

Lynch, D. C., and Rose, Marshall T. (1993). *Internet System Handbook.* Greenwich, CN: Addison-Wesley Publishing Company.

Makley, W. K. (1987). Computer Security's Worst Enemy: Management Apathy. *The Office, March 1987* (105:3), 115-116.

Manheim, M. (1993). Integrating global organizations through task/team support systems. In L. Narasim (Ed.), *Global Networks* . Cambridge, MA: MIT Press.

Mankin, D., Bikson, T.K., Gutek, B. (1984). Factors in Successful Implementation of Computer-Based Office Information Systems: A Review of Literature with Suggestions for OBM Research. *Journal of Organizational Behavior Management, 6 (3/4)*, 1-20.

Markus, M. L. (1983). Power Politics and MIS Implementation. *Communications of the ACM, 26 (6)*(June 1983), 430-444.

Martin, C. D. (1993). The Myth of the Awesome Thinking Machine. *Communications of the ACM, April, 1993*(36:4), 120.

Martin, C. D., Huff, Chuck, Gotterbarn, Donald, and Miller, Keith (1996). Implementing a Tenth Strand in the CS Curriculum. *Communications of the ACM, December 1996*(12:39), 75.

Martinko, M. J., Henry, John W., and Zmud, Robert W. (1996). An Attributional Explanation of Individual Resistance to the Introduction of Information Technologies in the Workplace. *Behaviour & Information Technology*(15:5), 313-330.

McAfee, J., and Haynes, C. (1989). *Computer Viruses, Worms, Data Dibblers, Killer Programs and Other Threats to Your System*: St. Martin's Press.

McCollum, T. (1997). Computer Crime. *Nation's Business, November 1997*(11:85), 18.

Meall, L. (1989). Survival of the Fittest. *Accountancy (UK), March 1989*(103:1147), 140-141.

Moore, G. C. (1987). End User Computing and Office Automation: A Diffusion of Innovations Perspective. *INFOR, 25 (3).*

Moore, G. C., Benbasat, I. (1991). Development of an Instrument to Measure the Perceptions of Adapting an Information Technology Innovation. *Information Systems Research, 2 (3)*, 192-222.

Morris, R., and Thompson, K. (1979). Password Security: A Case History. *Communications of the ACM*(2:11), 594-597.

Morshedian, D. (1986). How to Fight Password Pirates. *Computer, January 1986*(19:1).

Munro, N. (1996). Sketching a National Information Warfare Defense Plan. *Communications of the ACM, November, 1996*(11:39), 15.

Nance, W. D. (1995). Growing Pains and Successes in Transforming the Information Systems Organization for Client/Server Development. *Computer Personnel, 16 (1)*(January 1995), 11-19.

NetVital (1998). Network Security Survey. (Vol. 1998,): NetVital.

Network Wizards (1998). Internet Domain Survey. (Vol. 1998). Available online at http://www.nw.com.

Neumann, P. G. (1978). *Computer Security Evaluation.* Paper presented at the AFIPS, Arlington, VA.

Neumann, P. G. (1994). Expectations of Security and Privacy. *Communications of ACM, September, 1994*(37:9), 138.

Neumann, P. G. (1997). Identity-related Misuse. *Communications of the ACM, July 1997*(7:40), 112-.

Niederman, F., Brancheau, J.C., and Wetherbe, J.C. (1991). Information Systems Management Issues for the 1990s. *MIS Quarterly, December 1991*(15:4), 475-502.

Nonake, I. (1991). The Knowledge Creating Company. *Harvard Business Review, 69*(6), 96-104.

Office of Technology Assessment. (1987). *Defending Secrets, Sharing Data: New Locks and Keys for Electronic Information* (OTA-CIT-310). Office to Technology Assessment.

Office of Technology Assessment. (1994). *Issue Update on Information Security and Privacy in Network Environments*. Congress of the United States.

Orlinkowski, W. J., and Gash, D.C. (1994). Technological Frames: Making Sense of Information Technology in Organizations. *ACM Transactions on Information Systems, 12 (2)*(April 1994), 174-207.

Osborne, D. and Gaebler, T. (1992). *Reinventing Government*. Reading, MA: Addison-Wesley Publishing.

Perry, R. E., and Kramer, K.L. (1979). *Technological Innovations in American Local Governments/The Case for Computing*. New York: Pergamon Press.

Pinsonneault, A., and Rivard, S. (1998). "Information Technology and the Nature of Managerial Work: From the Productivity Paradox to the Icarus Paradox?" *MIS Quarterly, 22(3)*(September 1998), 287-311.

Porter, M. (1990). *The Competitive Advantage of Nations*. New York: Free Press.

Quinn, J. (1992). *Intelligent Enterprise*. New York: Free Press.

Reid, B. (1987). Reflections on Some Recent Widespread Computer Break-Ins. *Communications of the ACM, February 1987*(30:2), 103-105.

Rheingold, H. (1993). *The Virtual Community*. Reading, MA: Addison-Wesley.

Roach, S. S. (1991). "Services Under Siege: The Restructuring Imperative. *Harvard Business Review*. (September-October, 1991), 82-92.

Robey, D. (1977). Computers and Management Structure: Some Empirical Findings Reexamined. *Human Relations, 30 (11)*(November 1977), 963-976.

Robey, D. (1979). User Attitudes and Management Information System Use. *Academy of Management Journal, 22*, 527-538.

Robey, D., and Azevedo, A. (1994). Cultural Analysis of the Organizational Consequences of Information Technology. *Accounting Management and Information Technology, 4 (1)*(1994), 23-37.

Rogers, E. M. (1983). *Diffusion of Innovations, 3rd Edition*. New York: Free Press.

Rouse, R. A., and Hartog, Curt (1988). The New MIS Professional - Part 1. *Journal of Systems Management, May 1988*(39:5), 6-10.

Sakaiya, T. (1991). *The Knowledge Value Revolution.* New York: Kodanska International.

Schein, E. (1992). *Organizational Culture and Leadership (2nd ed.).* San Francisco, CA: Jossey-Bass Publishers.

Schell, R. R. (1979). Computer Security: The Achilles Heel of the Electronic Air Force. *Air University Review, January/February 1979*(30:2), 16-33.

Schwartz, H., and Davis, S. (1981). Matching Corporate Culture and Business Strategy. *Organizational Dynamics, 10 (1)*(Summer 1981), 30-48.

Senge, P. (1990). *The Fifth Discipline: The Art and Practice of the Learning Organization.* New York: Doubleday.

Shimomura, T., with Markoff, J. (1996) *Takeoff.* Hyperion Press, New York.

Smith, H. J. (1993). Privacy Policies and Practices: Inside the Organizational Maze. *Communications of the ACM, December 1993*(36:12), 105-122.

Spafford, E. (1989). Crisis and Aftermath. *Communications of the ACM, June 1989*(32:6), 2.

Spafford, E. H. (1991). Preventing Weak Password Choices. .

Stalk, G., and Hout, T. (1990). *Competing against time.* New York: Free Press.

Stoll, C. (1990). *The Cuckoo's Egg: Tracking a Spy Through the Maze of Computer Espionage.* Pocket Books.

Straub, D. W. (1989). Computer Abuse and Computer Security: Update on an Empirical Study. *Security, Audit, and Control Review, Spring 1986a*(4:2), 21-31.

Straub, D. W. (1990). Effective IS Security: An Empirical Study. *Information Systems Research, September 1990*(1:3), 255-276.

Straub, D. W., and Wetherbe, J.C. (1989). Information Technologies for the 1990s: An Organizational Impact Perspective. *Communications of the ACM, November1989*(32:11), 1328-1339.

Straub, D. W., Carlson, P.J., and Jones, E.H. (1993). Deterring Cheating by Student Programmers: A Field Experiment in Computer Security. *Journal of Management Systems* (5:1), 33-48.

Straub, D. W., Jr. (1990). Discovering and Disciplining Computer Abuse in Organizations: A Field Study. *MIS Quarterly* (March 1990), 45-55.

Suomi, R. (1996). One Size Fits All - or Does It? *Behaviour & Information Technology*(15:5), 301-312.

Szuprowicz, D. W., Jr. (1988). Technological Vulnerability: How Serious a Threat to Your Business. *Canadian Datasystems, October 1988*(20:10), 96-99.

Thompson, K. (1984). Reflections on Trusting Trust. *Communications of ACM, August 1984*(27:8), 761-763.

Thurow, L. (1992). *Head to head: The coming economic battle among Japan, Europe and America.* New York: William Morrow and Company.

Tornatzky, L. G., Klein, K.L. (1982). Innovation Characteristics and Innovation Adoption-Implementation; A Meta-Analysis of Findings. *IEEE Transactions on Engineering Management, EM29-1*(February 1982), 28-45.

Von Wodtke, M. (1993). *Mind over Media: Creative Thinking Skills for Electronic Media.* New York: McGraw-Hill.

Wade, J. R. (1989). Take It To The Top: Computer Information Security: Getting the Protection You Need. *Security Management, March 1989*(33:2), 7A.

WarRoom Research. (1996). *Information Systems Security Survey.* WarRoom Research. Available at http://www.warroom.com.

Wilkes, M. V. (1990). Computer Security in the Business World. *Communications of the ACM, April 1990*(33:4), 399.

Wilkes, M. V. (1991). Revisiting Computer Security in the Business World. *Communications of the ACM, August 1991*(34:8), 19-21.

Wood, C. C. (1987). Information Systems Security: Management Success Factor. *Computers & Security, August 1987*(4:6), 314-320.

Wood-Harper, A. T., Corder, Steve, and Wood, J.R.G. (1996). How We Profess: The Ethical Systems Analyst. *Communications of the ACM, March 1996*(39:3), 69-77.

Zmud, R. W. (1982). Diffusion of Modern Software Practices: Influence of Centralization and Formalization. *Management Science, 28 (12),* 1421-1431.

Zmud, R. W. (1983). The Effectiveness of External Information Channels in Facilitating Innovativeness Within Software Groups. *MIS Quarterly* (June 1983), 43-58.

Zmud, R. W. (1984). An Examination of the 'Push-Pull" Theory Applied to Process Innovation in Knowledge Work. *Management Science, 30 (6)*, 727-738.

Zuboff, R. (1988). *In the Age of the Smart Machine: The Future of Work and Power.* New York: Basic Books.

Vita

Cherie Long was born in Savannah, Georgia on January 11, 1961, the first child of Ray E. Long and Patricia Ann Thompson Long. As a youth she lived in Georgia, Florida, and Colorado. After graduating from Southwest High School in Macon, Georgia, she attended Mercer University in Macon, Georgia, and graduated with majors in Speech and Dramatic Arts and Political Science.

She returned to school in 1989 when she enrolled at the University of Central Florida and received a master's degree in Communication. After leaving UCF she began an interdisciplinary Ph.D program in Management Science and Information Systems, Radio, Television, Film (New Media Technologies) and Information Science. In the doctoral program her primary research concentrations were in new technologies, information security and digital commerce.

Permanent Address: 2180 West Ponce de Leon Avenue, Decatur, Georgia 30030

This dissertation was typed by the author.