# CONTROL MEASURES FOR DETECTING AND PREVENTING COMPUTER CRIMES.

A Research Topic
Presented to the Business Division
Beirut University College

In Partial Fulfillment of
the Requirements for the Degree
Master of Science in Business Management



BY
HOUSSAM MOHAMAD TABBARA
FEBRUARY, 1994

# BEIRUT UNIVERSITY COLLEGE
# P.O. BOX 98 13-5053
# BEIRUT , LEBANON

## APPROVAL OF RESEARCH TOPIC

CANDIDATE: HOUSSAM MOHAMAD TABBARA DATE: FEBRUARY 1994

DEGREE: MASTERS OF SCIENCE IN BUSINESS

ADVISOR: DR. TAREK MIKDASHI

TITLE OF RESEARCH TOPIC: CONTROL MEASURES FOR DETECTING AND PREVENTING COMPUTER CRIMES.

The following professors nominated to serve as the advisors of the above candidate have approved his research work.

ADVISORS

DR. TAREK MIKDASHI

NAME

[redacted]

SIGNATURE

DR. ABDUL RAZZAK CHARBAGI

NAME

[redacted]

SIGNATURE

# ACKNOWLEDGMENT

I would like to express my serious and deepest gratefulness to my advisor Dr. Tarek Mikdashi who, by his kind assistance, recommendations and serenity, has supervised the research through to completion. I would like also to reveal my gratitude to my second advisor Dr. Abdul Razzak Charbagi for his considerate guidance and the advises he supplied me with. My truthful gratefulness and appreciation to my dearest friend Manal Yunis for her consistent encouragement and motivation. Regards to all my friends who provided me with power to complete this research, Mohamad Tabbara, Imad Mirza, Kamal Mirza, Ramzi Mirza, Sana Kouwatli, Zeina Al Shami Arakji, Mirna Chamas, Rima Abou Fākher Eddine, Rima Bahous, and especially Rita Assaad for being so patient and tolerant.

Finally, my sincere love, and recognition for my parents, Mohamad, Samira, Rania, Dania and Moustapha, for their continuous support and believe in my person.

# TABLE OF CONTENTS

CHAPTER Page



CHAPTER Page

# CHAPTER I

## INTRODUCTION

### 1.1 General Overview.

One of the main functions of information systems is to enhance management's control over the operational, strategic, and decision-making activities of the organization. However, information systems themselves must be properly controlled to realize this objective. Without proper safeguards, systems are vulnerable to destruction, abuse, error, and loss, which can totally undermine the organizations that rely on them. Therefore, special measures must be taken during the design and operation of information systems to ensure that they are properly controlled.

In the past, the control of information systems was treated as final step, addressed only toward the end of implementation, just before the system was installed. Today, however, organizations are so critically dependent on information systems that vulnerabilities and control issues must be identified as early as possible. The control of an information system must be an integral part of its design. Users and designers of systems must pay close attention to control throughout the system's life span.

## 1.2 System Vulnerability and Abuse.

Before computer automation, data about individuals or organizations were maintained and secured as paper records dispersed in separate business or organizational units. Information systems concentrate data in computer files that can potentially be accessed more easily by large numbers of people and by groups outside the organization. Consequently, automated data are more susceptible to destruction, fraud, error, and misuse.

### Why Systems are Vulnerable ?

There are many advantages to information systems that are properly safeguarded. However, when large amounts of data are stored in electronic form they are vulnerable to many more kinds of threats then when they exist in manual form. Table I lists the most common threats against computerized information. They can stem from technical, organizational, and environmental sources[1].

---

[1] Kenneth C. Laudon & Laudon Jane Price, Management Information Systems, (N.Y.: Macmillan Publishing Company, 1991), P.729.

**Table I.**
**Threats to computerized Information Systems:**

| | |
|---|---|
| Hardware failure | Fire |
| Software failure | Electrical problems |
| Personal actions | User errors |
| Terminal access penetration | Program changes |
| Theft of data, services, equipment | Telecommunication problems |

Computerized systems are vulnerable to such threats for the following reasons:

- The development and operation of automated systems require specialized technical expertise, which cannot be easily communicated to end users. Systems are open to abuse by highly technical staff members who are not well integrated into the organization. For example, programmers and computer operators can make unauthorized purposes. Maintenance staff may make unauthorized copies of data files for illegal purposes.
- Although the chances of disaster in automated systems are no greater than in manual systems, the effect of a disaster can be much more extensive. In some cases, all of the system's records can be destroyed and lost for ever.
- Most automated systems are accessible by many individuals. Information is easier to gather, but more difficult to control.
- Data in computer systems undergo many processing steps than in manual systems, each of which is open to errors or

abuse. Each of these functions - data origination, recording, transmission or processing, processing, storage, retrieval and dissemination - requires a separate set of physical, administrative, and technical controls.

- On-line information systems are even more difficult to control because data files can be accessed immediately and directly through computer terminals. Legitimate users may gain easy access to computer data that were previously not available to them. They may be able to scan records or entire files that they are not authorized to view. By obtaining valid users' logons and passwords, unauthorized individuals can also gain access to such systems. The chances of unauthorized access to or manipulation of data are considerably higher than in the batch environment.
- Advances in telecommunications and computer software have magnified these vulnerabilities. Through telecommunications networks, information systems in different locations can be connected. The potential for unauthorized access, abuse, or fraud is not limited to a single location, but can occur at any access point in the network.
- Additionally, more complex and diverse hardware, software, and organizational and personnel arrangements are required for telecommunications networks, creating new areas and opportunities for penetration and manipulation.
- Advances in computer software have also increased the chances of misuse and abuse. Using fourth-generation

languages, for example, end users can now perform programming functions that were formerly reserved for technical specialties. They can produce programs that inadvertently create errors, and they can manipulate the organization's data for illegitimate purposes.

- Also, viruses can spread via computer networks and can invade computerized information systems from "infected" diskettes from an outside source or through infected machines. The potential for massive damage and loss from future computer viruses remains.
- Finally, the growth of database systems, where data are shared by multiple application areas, has also created new vulnerabilities. All data are stored in one common location, but many users may have the right to access and modify them. It may not be easy to identify who is using or probably misusing the data in such circumstances. Since the data are used by more than one organizational unit, the effect of an error may spread throughout the organization. There may also be less chance of discovering errors. Each functional unit has less individual control over the data and has less grounds for knowing whether the computer is right.

The increased vulnerability of automated data has created special concerns for the builders and users of information systems. These concerns include disaster, security, computer crime and abuse, and

administrative error. This research will deal with one of these concerns: Security.

## 1.3 Security.

An important concern that must accompany the planning of many MIS outputs is security. Which refers to "protection of computer-based resources - hardware, software, data, procedures, and people - against alteration, destruction, or unauthorized use."[2]

At one time security was relatively straightforward: Only a centralized mainframe needed to be guarded. The rise in communications networks compounded the security problem immensely since people became capable of accessing centralized data from a variety of locations. Within the last several years, a number of other threats to security have shown up. The rise in microcomputer-based processing, for instance, has distributed electronic data to scores of local sites, many of which have no security controls what so ever. Also, the surge in computer literacy has made it possible for ever more people to use computer systems to serve their own ends.

Figure 1-1 shows a number of security-related concerns. It is worth mentioning here that the overall responsibility for security lies with top management. The chief executive officers (CEOs) should know how vulnerable their organizations are to security problems and should assess

---

[2] Charles S. Parker, Management Information Systems, (N.Y: Mc Graw-Hill Publishing Company, 1989), P. 778

languages, for example, end users can now perform programming functions that were formerly reserved for technical specialties. They can produce programs that inadvertently create errors, and they can manipulate the organization's data for illegitimate purposes.

- Also, viruses can spread via computer networks and can invade computerized information systems from "infected" diskettes from an outside source or through infected machines. The potential for massive damage and loss from future computer viruses remains.
- Finally, the growth of database systems, where data are shared by multiple application areas, has also created new vulnerabilities. All data are stored in one common location, but many users may have the right to access and modify them. It may not be easy to identify who is using or probably misusing the data in such circumstances. Since the data are used by more than one organizational unit, the effect of an error may spread throughout the organization. There may also be less chance of discovering errors. Each functional unit has less individual control over the data and has less grounds for knowing whether the computer is right.

The increased vulnerability of automated data has created special concerns for the builders and users of information systems. These concerns include disaster, security, computer crime and abuse, and

the risk they are willing to tolerate. It is of course impossible, and certainly unfeasible, to make any system 100 percent secure; there will always be some element of risk involved.

**Fig. 1-1.** Sources of security problems

| | |
|---|---|
| ***Human carelessness:*** | |
| -Keying or input error. | -Program damaged during development or use. |
| -Computer operator error . | -Misplaced file or volume. |
| -Wrong version of program being used. | -Physical damage of I/O media. |
| ***Computer crime:*** | |
| -System sabotage. | -Sensitive data changed in an unauthorized way. |
| -Espionage. | -Program or data copied and used for unauthorized purposes. |
| -Using computer systems to steal money or goods. | |
| ***Natural or political disasters:*** | |
| -Fire, flood, or wind damage. | -Rioting or war. |
| ***Hardware & software failures:*** | |
| -Equipment malfunctions. | -Data damaged by hardware or software failures |
| -Power outages | -Undetected data transmission errors. |

**Source:** Parker, P.779.

## 1.4 The Need for The Study.

Changes in MIS technology have occurred concurrently with the expansion of both management and non-management information needs and requirements. Not only has the number of computerized management information systems multiplied, but new capabilities and user applications also have continually been developed and refined. These advances have had a number of implications for MIS management, especially in the area of auditing and control procedures. In effect, a great need exists for effective control over management information systems.

The need for this study stems from the fact that computer systems play such a critical role in business, government and other institutions, and that these organizations too must take special steps to ensure that their automated information is accurate, reliable, and secure. Automated information systems must be properly controlled if they are to serve the purposes for which they are intended. MIS management, therefore, must not ignore its responsibility for system controls, "but rather must get users as well as internal auditors involved in building the necessary controls at the design stage. This is opposed to the 'add-on approach' currently employed by many organizations. The involvement of the audit control functions in all phases of information systems is absolutely necessary and proper in today's more complex DP (data processing) environment, especially in the light of increasing computer crimes."[3] The growth of data communications to connect facilities at remote locations in a distributed data processing environment is one example of how new technology has complicated the control of computer crimes, not to mention normal DP problems and irregularities.

**Statement of Hypotheses:**

Thus research intends to study the following hypotheses:

- With the rise of communications networks and microcomputer-based processing, as well as with the general increase in computer literacy, security has become

[3] Robert J. Thierauf, Effective Management Information Systems, (Ohio: Bell & Howell Company, 1984), P. 341.

more difficult to manage effectively. Still management does not approach this issue as a serious problem.

- The risk of having computer crimes is highly associated to factors as employee morale and loyalty toward the company, size of the organization, span of control, age, and organizational level .

## 1.5 The Purpose of the Study.

The justification for management information systems organization is to provide services to the user. The manager must see that these services are developed in an appropriate manner, delivered at an acceptable cost, and operated effectively. That's why organizations should follow or adopt certain control methods and security measures to minimize risks and avoid threats in the MIS environment.

The study is based upon the premise that it is the management's responsibility to set effective security measures for the information that the organization uses or generates. Based on this, it intends to study the extent to which managers, working in organizations operating in Lebanon and belonging to various economic sectors, are aware of this responsibility and how they are applying it. Also, a description and an assessment of the various security methods, procedures and policies used will be portrayed.

It is worth mentioning here that the research will follow the following outline:

**Chapter II** will be concerned with reviewing the literature that dealt with the issue of security (including the various threats it should be established against, and the various control measures that should be adopted by information managers).

**Chapter III** will display the methodology followed to complete this study, and the various types of statistical analyses that will be applied to test the research hypotheses.

**Chapter IV** will list and explain the study findings based on the statistical analyses used.

**Chapter V**, Finally, will summarize the major study findings and will suggest certain recommendations concerning the issue of security management.

# CHAPTER II

## REVIEW OF LITERATURE

### 2.1 General Overview.

This is the information age. In a few decades, computing speed has increased several times in magnitude, the physical space required by computers has been reduced several times in magnitude, reliability has improved dramatically, and computers have been interconnected nationally and internationally through various communication links. Moreover, the cost of computing and the cost of interconnecting has decreased substantially. "In no other area have we approached this kind of performance increase and cost decrease."[4]

One of the implications of these improvements is that computers and computer communication links are now affordable and in the hands of more users. Most of us now use these capabilities, either directly or indirectly. This growth has significant security implications. A large number of individuals have personal computers, many of which can communicate through modems over ordinary telephone lines. Most businesses, small or large, depend on computers for accounting records, and payroll functions. Minicomputers have provided small companies with the same computing capabilities once affordable only by very large organizations. Dedicated microprocessors are now used as controllers to

4. James Arlin Cooper, Computer and Communications Security: Strategies for the 1990s, (N.Y.: Mc Graw- Hill Book Company, 1989), P.xv.

enhance the capabilities of calculators, telephones, microwave ovens, vending machines and cash registers. Financial transactions have been facilitated by computing links. Typing and editing are speeded by dedicated word processors and are available on most computers.

Application software such as graphics generators, spreadsheet packages, database systems, and computer aided design aids is easily affordable and readily available for all sizes of computers. People who never thought they would use a computer are becoming dependent on these powerful computer functions.

However, two general threats reduce the excitement of these developments. "One of these threats are persons who watch for security weaknesses on which to capitalize. Frequently, new technological developments have substantially improved opportunities for these people. The second general threat is what may appear to be a random occurrence. It is important to recognize that many things can go wrong due to human mistakes, malfunctions, accidents and natural disasters."[5] Many argue that this latter class of threat is the most serious current problem organizations face. In any event, both classes of threat are important.

It is known that the present environment has many new security problems. Some of them are obvious. The down loading and general distribution of confidential, private, and proprietary information to

---

5. Ibid, P.xvi.

individual work stations makes it more difficult to assure protection of these sensitive data.

The pervasiveness of communication links within buildings and around the world via phone lines, hard-wired connections, and electromagnetic transmission exposes the information to active or passive tapping and to interference in the form of modification, replication, and deletion. The potential sophistication of some of the new attach methods (especially the virus) has led to warnings that the way in which computing is done may have to undergo significant changes in the future.

Information processing is changing. Information stored in modern storage media is packed so densely and is so transparent to the observer that its reading or movement becomes hard to control[6]. For example, many libraries and businesses control unauthorized removal of books and other documents by visual observation. The amount of information in a number of books could, if written on diskettes, fit in a pocket.

A new problem has developed in the sale of applications software. A diskette or similar storage medium containing proprietary applications programs may represent a very small production cost. However, the information contained on it may represent a substantial program development cost. Companies marketing software are therefore

---

6. Ibid, P.xvii.

faced with a hard security problem. They would like their product to be easy to use, ease to transfer to a hard disk, and easy to copy for a backup. However, illegal copying (software piracy), which can deprive software suppliers of considerable income, should be made very difficult. Threats to computer integrity include vandalism, sabotage, terrorism, hardware failures, and software bugs. That's why the technology available in the present time should contribute to the computer and communications security threat environment.

This chapter will shed the light upon the researches that were made in the area of computer security and about the various security measures that could be adopted by computerized organizations to make their computer work more efficient.

## 2.2. Information Security and Privacy.

Security and privacy nowadays are major issues addressed immensely by many researches and book authors. The trend toward personal computers, local area networks, and end user programming - and away from centralized centers and professional programming - can make companies more vulnerable to electronic intrusion. The continued rapid growth in end user computing will increase the risk in both security and privacy to the point where management must directly address these issues. In fact, security is a major challenge in the management of distributed systems, which led currently to a major emphasis on preventing the criminal misuse of computers.

The increasing use of distributed systems will further complicate the security issue. Therefore, as computers are moved out from secure computer centers to insecure offices, vulnerability to computer crime will probably increase[7]. How should information systems management deal with this new vulnerability ? Can the responsibility for computer security be passed on to user department management, along with the machines? If so, how should the responsibilities be split between the information systems department and user management ? These are the questions that are addressed here.

### 2.2.1 New Vulnerabilities.

Among the features of distributed systems that will lead to new vulnerabilities are[8]:

- Distributed equipment.
- Distributed data.
- Distributed programs.
- Distributed knowledge of computers
- Distributed program documentation.
- Distributed printed forms.

This distributed environment is much different from a centralized system. Distributed systems move the actual processing capability to various locations. In the central system, the information systems

7. Ralph H. Sprage & McNurlin, Barbara C., Information Systems in Practice, (New Jersey: Prentice-Hall, Inc., 1986), P. 131.

8. Ibid, p.p. 130 - 131.

department controls the terminal network and must, therefore, also control security. Whereas in the distributed system, many of the data processing components are no longer under the physical control of the information systems department. In addition, there may not be much conformity among the numerous departmental systems. Therefore, the information systems department's role would be to guide user departments and help them create plans for equipment selection, software development, work scheduling, and security.

### 2.2.2. New Threats.

Under a central batch system, it has been easiest to:

1. Insert false input through the regular data entry mode.
2. Steal master file data, for example, by walking out with a tape (or diskette), copying it elsewhere and returning it.
3. Steal services, such as operating the machine at night for private purposes.
4. Damage equipment.

These are the "big four" reported computer crimes[9]. They are considered the big four because they may well be the easiest to perform in a centralized batch processing environment. When terminals in remote locations are added -with easier access and fewer controls- an intruder can do all what is mentioned above, as well as

5. Change programs.
6. Change master files.

---

9. Ibid, p.p. 132.

7. Alter input.

Given the distributed system environment, it is most likely that new threats that endanger a company would appear. Figure 2-1 summarizes the threats to which a distributed system is susceptible.

**Fig. 2-1**. Threats in a Distributed Environment

| **THREATS INVOLVING THEFT** |
|---|
| Steal master file<br>Steal computer Time<br>Steal output<br>Steal equipment |
| **THREATS INVOLVING DESTRUCTION** |
| Destroy equipment<br>Destroy data Files |
| **THREATS INVOLVING MANIPULATION** |
| Insert false input<br>Suppress certain output<br>Alter output<br>Alter master file<br>Modify a program<br>Damage or modify Equipment |

**Source:** Sprague & Mc Nurlin, Information Systems Management in Practice, P. 133.

## 2.3 Managing Computer Security.

Although there is a big concern about computer security, few empirical studies have been made of computer crime, fraud, and abuse, computer security control and audit, and the cost of security. In certain

studies that have been made, there was no comparison between the ways firms actually manage their security and the way they admit they should.

However, a survey was conducted by Farhoomand and Murphy[10] about the fortune 500 firms to gain insight into the nature of various elements of computer security management. An attempt was made to investigate relationships between the prevailing computer security problems and the size of a company's information systems facilities, as measured by the number of MIS employees and the annual budget of the MIS department.

After mailing the surveys inquiring about various aspects of computer security to computer security officers or MIS managers of all the Fortune 500 companies, it was found by the researchers that the median annual MIS budget of the responding companies had been estimated to be approximately $20 million. More than half of the respondents allocated less than 0.5% of this to computer security; about a third allocated between 0.5% and 1.0%; and the remaining companies allocated more than 1.0% .

Concerning policy direction, standards and procedures, and areas of responsibility, the surveyed firms responded that they had comprehensive guidelines in place. More than three quarters of the firms have documented emergency, backup, and recovery plans. However,

---

10. Ali F. Farhoomand, "Managing Computer Security", Datamation, Vol. 10 No. 5, January 1, 1989, p.p. 67-77.

approximately one third of the firms never test these plans, nor do they reevaluate security programs at specified intervals. It was also reported that policies are generally formulated by consultation between the MIS manager and top management. Before computer security policies can be adopted, final approval must be obtained from senior management. Such an involvement in both policy setting and approval indicates that top management provides a high level of support to the computer security program.

Another important finding in the survey is that personnel security programs are weak. In particular, it was reported that firms do not:

- Use attitude surveys to test the level of employee morale.
- Consider an employee's level of security consciousness during his/her performance evaluation.
- Use job rotation as a means of evaluating an employee's security-related behavior.
- 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.

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. Moreover, it was found out that slightly more than half of the firms have developed asset-threat inventories; i.e., inventories that address what safeguards will 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 rest of the firm neither perform any risk assessment of security threats nor do they formally identify and evaluate their computer assets. Subjective methods are widely used in identifying assets and evaluating potential threats than quantitative methods such as the Delphi technique or threat model- an analysis tool for identifying threats that is based on cause and effect relationships. In fact, "risk analysis need not be performed to know that software security systems are required. In fact, such analysis only prove what is already known and, thus, amount to wasted time and effort."[11]

The overall finding of this survey is that security officers felt that still more can be done to enhance the level of security within their firms, and they recommend applying more formal analysis and control procedures to security programs, as well as increasing the frequency of a certain security procedures. The problems that have affected the largest number of firms are summarized and shown in table II.

---

11. Ibid, p.p.68.

**TABLE II**
**Problems affecting Computer Security**

| PROBLEM | % FIRMS AFFECTED |
|---|---|
| Utilities failure | 80.8 |
| Inadequate control | 75.6 |
| Compliance failure | 73.1 |
| Improper guidance | 67.9 |
| Environment support breakdown | 64.1 |
| Electromagnetic discharges | 43.6 |
| Liquids | 29.5 |
| Electronic intrusion | 29.5 |
| Fraud & embezzlement | 16.7 |
| Gases | 11.5 |
| Extreme temperature | 11.5 |
| Physical intrusion | 10.3 |
| Service loss | 7.7 |
| General violence (Vandalism) | 7.7 |
| Specific violence (sabotage) | 6.4 |
| Living organisms | 2.6 |
| Projectiles | 2.6 |
| Earth movements | 1.3 |

**Source:** Farhoomand, Managing Computer Security, Datamation, Vol. 10, No. 5, p.p. 68.

The costliest are utilities failure according to 36% of the firms: compliance in 33% of the firms; and improper guidance, in 21% of the firms. These findings according to the survey, suggest that the often publicized threats such as computer hackers and white collar criminals have had either little or no effect on the majority of firms, or are not being reported.

Another survey was conducted by the National Center for Computer Crime Data (NCCCD) in Los Angeles of 3,500 Computer Security Professionals and reported by J.J. Bloombecker[12] detailed in types of computer crime:

- money theft
- information theft
- damage software
- malicious data alteration
- deceptive data alteration
- theft of services
- harassment
- extortion, and
- damage to hardware.

Telephone services were the most common service theft with computer services constituting much of the remainder. According to Blommbecker, these are types of computer crime. Referring to a study made by Donn Parker, a leading computer security consultant, Bloombecker stated the

---

12. J.J. Bloombecker, "Short- Circuiting Computer Crime", Datamation, Vol. 11, No. 6, October 1, 1989, p.p. 71-72.

set of generally used controls that should be present in every well-run computer center. These are shown in table III. In fact IS (information system ) managers should consider adopting some or all of the seven types of these general computer security controls.

Other practices include the separation of duties, such as preventing application developers from administering the application, and using daily code words for voice communication systems. Moreover, It was found that top management commitment to security as the most important and valuable component of a general security strategy. Other components of security strategy ranked in order of importance by NCCCD's survey respondents are: (1) Establishing corporate ethical norms for computer use, (2) Maintaining employee awareness and training, (3) Enforcing computer crime laws, (4) Securing communications and electromagnetic emanations, (5) Controlling physical access, (6) Using smart cards, advanced encryption, intrusion detection expert systems, secure networks and anti virus products.

According to the center's director of research, the result of this survey " Demonstrate what others are doing to protect against various types of computer security violations. There is no escaping the need to keep abreast other managers' practices, particularly those with similar vulnerabilities or in the same industry"[13].

---

[13]. Ibid, p.p. 72.

**Table III**

**The well-Secured Computer Center.**

| Security controls to be adopted by IS managers: |
|---|
| * Manual assurance of data integrity-destroy discarded documents, eliminate incomplete and absolute data. |
| * Physical security- keep a low profile for the computer center prohibit smoking and eating in some computing areas. |
| * Operations security- isolate sensitive computer production duties, protect data used in system testing, set up disaster recovery policies, document courier trust worthiness and identification. |
| * Management- initiated controls- appoint a computer security management committee and officer, keep security reports confidential. |
| * Computer program development and maintenance controls- set up quality assurance procedures and access control for programming library. |
| * Computer system controls- set up technical review of operating system changes, cryptographic protection and input data validation. |
| * Computer terminal access controls-set up terminal and protocols for login. |

**Source:** (Bloombeker, 1989) from: Computer Security Techniques (U.S. Department of Justice).

## 2.4. Increased concern about Computer Security.

Awareness of the importance of end-user authentication (credibility) to better protect organizations from unauthorized computer access is increasing. A survey conducted by Ernest and Whinney of computer security specialists[14] concluded that new methods to ensure the

14. Ernest & Whinney, "Concern about Computer Security Increasing", Journal of Accountancy, Vol. 18, No. 3, June 1987, p.p. 26-28.

confidentiality and integrity of information "based on encryption technologies for telecommunications, file storage and message authentication are needed. And the nature of contingency planning will continue to evolve, becoming more of a total organization effort instead of a data processing concern."[15]

The survey was conducted among more than six hundred registrants at the Computer Security Institute's annual conference. 68% of the respondents indicated that organizations continue to recognize the increasing importance of security issues. In addition, 62% of the respondents believe that security risks are rising, and 75% are taking substantial steps to implement security policies. However, only 6% said that the safeguards taken by their organizations against security risks were completely adequate. Furthermore, less than half (42%) of the organizations have information and computer security orientation programs for new employees. Moreover, the competition, employees and foreign governments (for both governments and industry) were ranked as the top groups from which respondents want to protect their organization's information. Survey results indicate the "hackers", those outside the organization who access confidential information for fun or profit, are perceived to be an embarrassment or threat to security, but not as serious a threat as commonly believed.

---

[15]. Ibid, p.p. 27.

An analysis of this survey states that the "emergence of competition as a major concern is relatively new trend. Historically, the security perspective grew from the audit perspective. That is, the major threat came from internal, unauthorized access to critical information from employees. However, in this year's survey, business and industry identified their competition as the top group from which their information must be protected."[16]

Concerning importance of certain security issues, data classification and network security were identified as the primary security issues facing both the public and private sectors. Network security was ranked higher by non government than government organizations. Network security usually includes protection of computer networks and computer applications from authorized and unauthorized users, message confidentiality and integrity, and end user authentication. Most respondents said that contingency planning is as important to their organizations as data integrity and confidentiality.

Ernest and Whinney concluded that apparently organizations recognize that service interruptions and the lack of contingency plans for them will impact their operations in terms of lost time, business opportunities and revenues, and has an organization wide impact.

---

16. Ibid, p.p.27.

In his article, "Computer/Technology: Protecting Mainframe Data from PCs"[17], J.L. Boockholdt stated that "It is not maliciousness that threatens the data; It is employees' sloppiness or incompetence. Each time an employee calls up a file and makes a change in a mainframe's data, an opportunity is created for introducing error. It makes no difference how innocent the error is; The file is corrupted"[18]. To guard against these dangers, certain ways may help, such as keeping unreliable employees away from the organization's PCs and carefully training all users. But in day-to-day office life, these steps usually aren't enough to solve the problem.

According to the author, the simplest and most effective security method is to prohibit a physical connection between a PC and the mainframe. If the user needs a file from the mainframe memory, an information manager downloads (copies) it into a floppy disk and delivers the disk by hand to the PC user. Later, before the file is returned to the mainframe -again by copying it onto the floppy- the data are scrutinized for errors.

Only when the new data are certified correct is the restored to the main frame. Although this procedure is inefficient, it was reported that some organizations rely on the technique to deal with sensitive data or as a security measure to be used until a more sophisticated network program

---

17. J. L. Boockholdt, "Computers/Technology: Protecting mainframe data from PCs", Journal of Accountancy, Vol. 8, No. 4, April 1991, p.p. 87-90.

18. Ibid, p.p. 87.

can be installed. Another technique is to program all critical files in the mainframe as " read-only". That's an operating system procedure that allows a file only to be read -not changed. However, a computer user with a certain knowledge of DOS can overcome this restriction. Also, the command limits employees' efficiency and the type of work they can perform on the computer. Moreover, a more effective way to protect mainframe data from PC users is with specially designed software that is generically called the PC-mainframe link.

Whatever the technology used is, certain minimum security procedures should be applied to all critical or sensitive data. For example, all authorized users should have passwords and user IDs stored in the mainframe. These codes should identify which mainframe databases are accessible to each PC user. The mainframe security program should record any attempt made by unauthorized user to access data files, execute sensitive programs or access utilities that make it possible to copy, modify or access files. After that, all such attempts should be investigated.

Whatever the technique used is, it is important to remember that "no network security system is foolproof. Even military networks have been compromised by hackers. But most sources of data corruption are not so clever or determined. A majority of problems are caused not by malicious interlopers, but by innocent but careless users."[19]

---

19. Ibid, p.p. 90.

## 2.5. Threats to Information Systems.

Information systems security remains high on the list of key issues facing information systems executives. In the review of literature made by Loch, Carr, and Warkentin[20], it is reported that many 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[21]. The reliance on computer and telecommunication systems has redefined corporate risk. As mentioned in the review of literature, management now recognizes that threats to continuing operations include technological issues seldom previously considered[22]. A survey done by Carter of U.S insurance companies found that 90% of these firms which are dependent upon data processing systems would fail after a significant loss or disruption of the EDP facility[23]. Protecting the corporation's information system and data well deserves management's attention.

---

[20].Karen Loch, Houston Carr. & Merill E. Warlentein, "Threats to Information Systems: Today's Reality, Yesterday's Understanding", MIS Quarterly, Vol. 16, No. 2, June 1992, p.p. 173-186.

[21]. L. Meall, "Survival of the Fittest"' Accountancy, UK, Vol. 103, No. 1147, March 1989, p.p. 140-141.

[22]. B.O. Szuprowicz, "Technological Vulnerability: How Serious a Threat to your Business?", Canadian Datasystem, Vol. 20, No. 10, October 1988, p.p. 96-99.

[23]. R. Carter, "Dependence and Disaster: Recovering from EDP Systems Failure", Management Services, UK, Vol. 32, No. 12, Dec. 1988, p.p. 20-22.

The review of literature made by the researches also showed that management's concern with information systems security has changed over recent years. In 1981, it ranked at the 14th most important information management topic[24]. By 1985, it had moved to the fifth place[25], but a 1986 study reported security in the 18th place[26], by 1989, the issue had dropped to the 19th place[27], probably indicating that the MIS executive believed that either that security was less of an issue, or they have implemented greater control. However, a major study conducted during 1989-1990 by the National Research Council concluded that, "The state of computer security in the USA is a mess"[28].

Risk, according to the dictionary, is "the possibility of loss or injury" and "the probability of such loss" (Merriam - Webster, 1989). Risk includes threats, resources, modifying factors, and consequences[29]. The components of threats are illustrated in fig. 2-2. Multiple forces exert

---

24. L. Ball and R. Harris, "SMIS Member: A Membership Analysis", MIS Quarterly, Vol. 6, No. 1, March 1982, p.p. 19-38.

25. C. Hartog and Herbert M., "1985 opinion Survey of MIS Managers: Key Issues", MIS Quarterly, Vol. 10, No. 4, Dec. 1986, p.p. 351-361.

26. J.C. Brancheau and Wetherbe J.C., "Key Issues in Information System Management", MIS Quarterly, Vol. 12, No. 2, March 1987, p.p. 23-36.

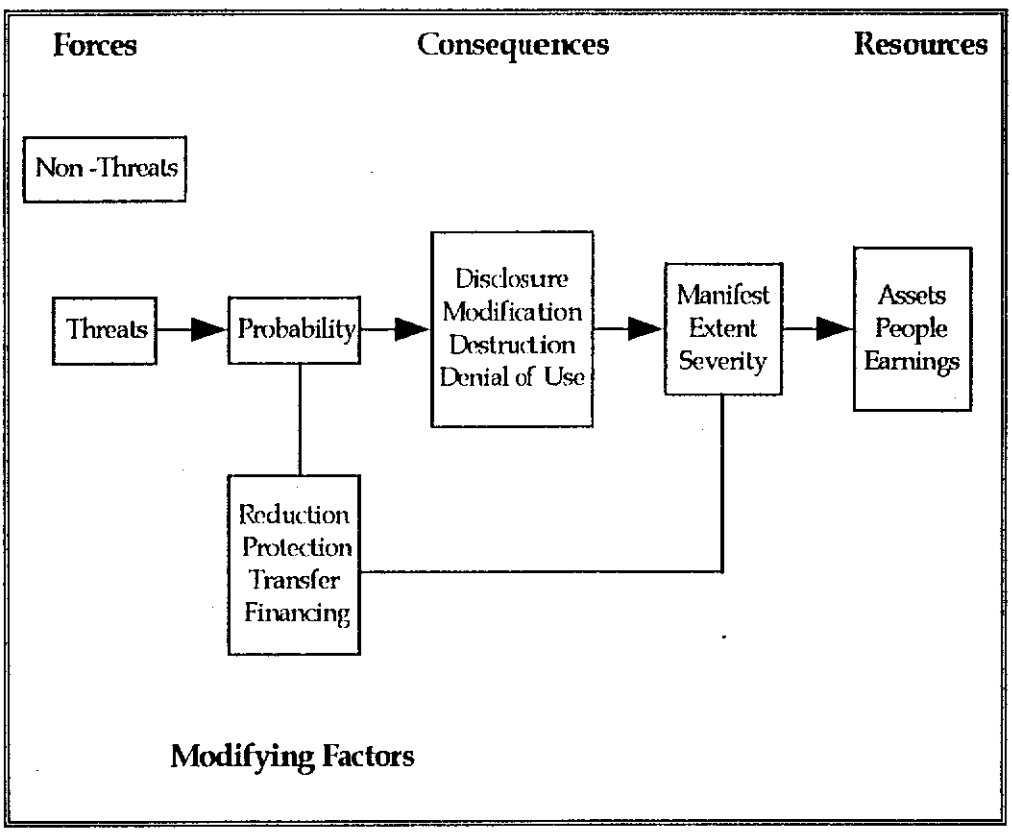
27. F. Neiderman, Brancheau J.C., and Wetherbe J.C.," Information Systems Management Issues of the 1990s", MIS Quarterly, Vol. 15, No. 4, December 1991, p.p. 475-502.

28. National Research Council, Computers at Risk, National Academy Press, Washington, DC, 1991.

29. N. Cockford, An Introduction To Risk Management, Cambridge: Woodhead, Faulkner Ltd., 1980.

influence on the organization; Threats are a broad range of forces capable of producing adverse consequences. Resources consist of those assets, people, or earnings potentially affected by threats. Modifying Factors are the internal and external factors that influence the probability of a threat becoming a reality or severity of consequences when the threat becomes a reality. Consequences are the ways a realized threat impacts the resources.

**Fig. 2-2.** The Components of Risk.




**Source:** Loch, Carr, & Warkentin, "Threats to Information Systems", MIS Quarterly, P.175.

Table IV categorizes these threats by source and perpetrator. A threat can be internal to the organization as a result of employee action or failure of an organizational process, or from the external environment. The most obvious external threats to computer systems and the resident data are natural disasters: Fire, floods, earthquakes, etc. Wide uses of telecommunications pose a threat of different type, access to internal data from external sources by competitors and computer hackers. A recent, growing threat that has received considerable attention is the computer virus.

Next, actions of the perpetrator (human versus non-human) may be accidental or intentional, irrespective of the source. Competitors typically would be interested in information access, while hackers' behavior may cause the full range of consequences. Also, computer viruses and program problems are differentiated by their creators' intent. Computer viruses are defined as malicious software written to produce an undesirable effect to the system, user, or organization. Whereas, program problems are most commonly the result of oversights by programmers/analysts.

**Table IV**
**Sources & Perpetrator of Threats to Information System Security.**

| SOURCE | HUMAN | NON-HUMAN |
|---|---|---|
| Internal Threats | -Acts by employee.<br>-Administrative procedures. | -Program problem.<br>-Mechanical & Electrical failures. |
| External Threats | -Competitors.<br>-Hackers. | -Natural disasters.<br>-Computer viruses. |

**Source:** Loch, Carr, & Warkentin, "Threats to Information Systems", MIS Quarterly, P.178.

The two major questions that were addressed by researchers were: (1) What are the threats to information systems and resident data? and (2) Which of these are the most serious threats?

Twelve threats were listed, respondents were asked to "rank the top three of the following (12) threats to the security of your organization's information system(s), for microcomputers, mainframes, and networks".

**Fig. 2-3** Threats to information systems security.

| MICRO-COMPUTER | MAIN-FRAME | NETWORK | THREATS |
|---|---|---|---|
| ******** | ******** | | Accidental entry of bad data by employees |
| ******** | ******** | | Intentional entry of bad data by employees |
| ******** | ******** | | Accidental destruction of data by employees |
| ******** | ******** | | Intentional destruction of data by employees |
| ******** | ******** | | Unauthorized access to data/system by employees |
| ******** | ******** | | Inadequate control over media (disks, tapes) |
| ******** | ******** | | Poor control over manual handling of I/O |
| ******** | ******** | ******** | Access to data/system by outsiders (hackers) |
| ******** | ******** | ******** | Access to data/system by outsiders (competitors) |
| ******** | ******** | ******** | Entry into system of computer viruses, worms |
| ******** | ******** | ******** | Weak, inadequate, physical control |
| ******** | ******** | ******** | Natural disaster: fire, flood, loss of power, communications |
| ******** | ******** | ******** | Others: |

**Source:** Loch, Carr, & Warkentin, "Threats to Information Systems", MIS Quarterly, June 1992, P.177.

Results reported, as shown in Figure 2-3, indicate that the first seven threats were of concern for microcomputer and mainframe computers only, whereas the last five threats were also appropriate for networks. Three methods of analysis were used: weighted votes, the number of first -place votes, and unit votes- to describe the overall meaning of including a threat in any of the three positions.

The findings of the research showed that the respondents are deeply involved with telecommunications, yet they don't seem to connect conceptually the level of connectivity (increased number of points of entry into the system) and level of risk. while they differentiated between stand-alone and connected environments, they viewed their internal networks to be relatively secure. Furthermore, although they acknowledged the potential risk for external networks, respondents perceived themselves to be at low risk. Their low level of concern was explained by the researchers by several factors. first, most of their external networks involved mainframe systems which they believed were secure. Second, informal comments suggest that they believe that the mainframe environment to be impervious to the threat of computer viruses, the thing that indicates a lack of awareness on their part.

Findings also reveal that respondents seemed well aware of the threats but viewed their risk to be moderately low. They also believed that their employees and competitors operate in good faith; intentional actions were consistently ranked as the least likely threats. Furthermore, they viewed their neighbor to be at a greater risk than they were,

exhibiting a rather naive belief that bad things only happen to other people.

Finally, regarding preventive measures against computer viruses, respondents were asked to rank possible actions designed to prevent infection by computer viruses, worms, etc. Table 2-5 shows that passwords, regular backups and employee education are by far believed to be the most effective preventive measures for viruses, and 2% of the responding organizations conducted ethics training.

**Table V**
**Ranking of Preventive Measures Against Computer Viruses.**

| VIRUS INFECTION PREVENTIVE MEASURES | VOTES | MEAN | STAND. DEV. | UNIT VOTES |
|---|---|---|---|---|
| -Use of passwords | 136 | 2.34 | 0.78 | 58 |
| -Backup procedures schedules | 84 | 1.83 | 0.71 | 46 |
| -Employee education | 75 | 2.27 | 0.84 | 33 |
| -Consistent security policies | 57 | 1.97 | 0.91 | 29 |
| -Company provided software | 50 | 2.08 | 0.83 | 24 |
| -Use of virus scanning software | 42 | 1.91 | 0.81 | 22 |
| -Audit procedures strengthened | 42 | 2.00 | 0.77 | 21 |
| -Monitor computer usage | 28 | 1.56 | 0.70 | 18 |
| -Auto terminal/ account logoff | 24 | 1.71 | 0.83 | 14 |
| -Shrinkwrap software only | 26 | 2.00 | 0.82 | 13 |
| -No outside BBS connections | 28 | 2.55 | 0.69 | 11 |
| -Publish formal standards | 19 | 1.73 | 0.79 | 11 |

**Table V** (continued)

| VIRUS INFECTION PREVENTIVE MEASURES | VOTES | MEAN | STAND. DEV. | UNIT VOTES |
|---|---|---|---|---|
| -Reporting violations encouraged | 19 | 1.90 | 0.74 | 10 |
| -Control of Workstations | 7 | 1.40 | 0.55 | 5 |
| -Other | 6 | 2.00 | 1.00 | 3 |
| -Ethics training | 5 | 1.67 | 0.58 | 3 |

**Source:** Loch, Carr, & Warkentin, "Threats to Information Systems", MIS Quarterly, P.184.

It is worth mentioning that the scale and methodology in this article will be applied or followed in this study.

Ch. 2 was a review of all the literature pertinent to the field of security. Ch. 3 Will show the methodology and design of this research.

# CHAPTER III

## RESEARCH DESIGN AND METHODOLOGY

### 3.1 The Basic Approach.

This research has been conducted in an attempt to unveil crucial factors related to computer crimes in Lebanon, specifically in the following industries: Banking, Education, Aviation, and Advertisement. Moreover, this survey seeks to assess and determine the various methods and measures that can be adopted to minimize these crimes and to increase computer security within these industries.

### 3.2 Sources of Information and Survey Design.

The sources of data gathered for this study are employees working in Lebanese organizations involved in Banking, Education, Aviation, and Advertisement and operating in Lebanon. The respondents belong to different management levels; Moreover, they are exposed to computers as an essential part of their job.

The survey, based on the basic methodology, has been designed to cover different factors related to computer crimes and computer security. The questionnaire, applied in this research, is divided into various parts including demographic characteristics, computer use, computer training, computer knowledge and experience, information system management, threats to information systems security, computer viruses relative to other threats, computer viruses prevention, beliefs about

computer threats and crimes, organizations' policies and measures, management and electronic data processing (EDP) support, and finally career and job attitudes. A sample questionnaire appears in appendix A. Responses item questions have been used to collect scores for these variable measures. The validity of the scales had been previously tested and verified by other researchers, who used these as the main tool for data collection, such as Mansour and Watson[30], Igbaria[31], and Srinivasan[32].

### 3.3 Sample and Data Collection.

Eight advertising agencies, eleven banks, two universities and one Airway company were approached by this survey for collection of data. These are computer using organizations in Lebanon. The questionnaire was distributed after having secured the approval and permission of top management.

One hundred and fifty questionnaires were prepared; However, only one hundred and seven were precisely distributed to managers and professional staff, since no more qualified respondents could be detected. Only 77 questionnaires were completed and returned. In order to prevent misapprehension of any question due to some difficult and technical

---

30 Ali H. Mansour & Hugh J. Watson, "The Determinants of Computer Based Information System Performance", Academy of Management Journal, Vol. 23, No. 3, 1980, p.p. 521-533.

31 Magid Igbaria et al., "Microcomputer Applications", Information & Management, Vol. 16, 1989, p.p. 187-196.

32 Ananth Srinivasan, "Alternative Measures of System Effectiveness", MIS Quarterly, Vol. 9, No. 3, September 1985, p.p. 243-258.

concepts used in the questionnaire, the process of personal approach was used by meeting with the respondent, explaining the purpose of the study and these technical concepts, then arranging another visit to explain questions that might not be clear to the respondent, and pick up the questionnaires. Nevertheless, 7 of these were disregarded due to missing and incorrect data, the rate of response was 65.42%.

The respondents came from a broad variety of organizations belonging to various economic sectors and from an extensive spectrum of management levels and functional divisions. In conformity with Yaverbaum[33], a former researcher in this field, one can conclude that the sample used seems to portray a fair representation of computer users for this area and can be considered as actually illustrative of an entire spectrum of attitudes and beliefs.

## 3.4 Measurement of the Model Variable.

The listed below subsections represent the measurement of the factors relevant to computer crimes and computer security. These were used in the design of the questionnaire displayed in appendix A.

### 3.4.1 Demographic Variables.

Single item questions were used to determine respondent's gender and age, years of education, years spent in this organization, number of subordinates reporting to each, total number of employees in

---

33 Gayle J. Yaverbaum, "Critical Factors in the User Environment", MIS Quarterly, Vol. 12, No. 1, March 1988, p.p. 79.

the organization, the budget spent on data processing, and the budget spent on instruments for securing these data. Furthermore, questions were posed to inquire about the functional area to which the respondent belongs. Eleven categories were used: accounting, finance, engineering, general management, personnel, information system, sales, manufacturing/production, marketing, R&D, and other to specify. Questions about the level of the respondent in the hierarchy level of the organization varied from Professional staff, First level supervisor, Middle management, Strategic management, and other to specify. Finally, The primary organization's business varied from manufacturing, utility, merchandising, public sector, health care, insurance, educational, financial services, and other to specify.

### 3.4.2 Computer Use.

List of questions were asked to identify the type of computer system used by the respondent, and the frequency of use. Frequency of hour use during a day was calculated by providing ranges from 0 under 2, 2 under 4, 4 under 6, and 6 under 8 hours per day. For the frequency of daily use during a month, the ranges were from 0 under 5, 5 under 10, 10 under 15, 15 under 20, 20 under 25 and 25 under 30 days per month.

### 3.4.3 Computer Training.

Computer training was measured by individuals' responses to questions inquiring the extent of training received from four sources: General courses at college or university, vendors and outside consultant, in-house company courses, and through self study. The responses option

ranged in a Likert-type scale from (1), "None", to (5), "Extensive". This was used by Igbaria et al. (1989) based on the proposition of Nelson and Chenny[34]. Igbaria had proved the validity of this scale since it had an internal consistency reliability of 0.86. The mean of the responses was used as the measure for this issue.

### 3.4.4 Computer Knowledge and Experience.

Four questions were used to estimate the actual experience of the respondents in working with computers and his knowledge about computers in general. The first question investigated the number of computer courses taken by the respondents, the second, the years spent in using PCs, the third, the years spent using computers in general, and finally, the years spent writing programs in computer language. The mean of the responses was used as the measure for this issue.

### 3.4.5 Issues for Information System Management.

Respondents were asked to rank the top 3 of 10 Information System Management issues according to their importance in order to evaluate the main three issues that Lebanese managers believe that information systems management should provide. Responses were coded 1, 2, and 3 for the top three respectively and 0 was assigned for the 7 remaining issues not ranked.

---

[34] R. Nelson and P. Cheney, "Training End Users: An Exploratory Study", MIS Quarterly, Vol. 11, No. 4, December 1987, p.p. 574-559

### 3.4.6 Threats to Information Systems Security.

Respondents were also asked to rank the top 3 of 12 issues that they presume are the most threatening to computer security. This ranking provided the study with the most serious threats to computer security in Lebanon. The same method of coding used in the previous section was used here.

### 3.4.7 Computer Viruses Relative to other Threats.

A set of questions was asked to calculate the frequency of virus infection faced by Lebanese organizations and the risk of computer disruption on information system due to the intrusion of computer viruses. Furthermore, one question tested the organizations' concern about the topic of virus intrusion.

### 3.4.8 Computer Viruses Prevention.

This measure was used to appraise the knowledge of each respondent about the major procedures that can be used to prevent computer infection by viruses and the extent to which the organization, he/she belongs to, apply these actions.

This measure is assessed by asking the respondents to indicate their agreement or disagreement with fourteen statements reflecting the major actions that can be used to prevent Viruses infection.

The responses options ranged in a Likert type scale from (1), "Not at All", to (5), "To a Great Extent". The mean of the responses was used as the measure for this issue.

### 3.4.9 Beliefs about Computer Threats and Crimes.

In this section of the questionnaire, 5 questions were asked to rate the respondents convictions about the present state of computer crimes. The responses options ranged in a Likert type scale from (1), "Strongly Agree", to (5), "Strongly Disagree".

### 3.4.10 Preventive Procedures Followed.

The ten questions of this section were utilized to evaluate the various measures used by Lebanese organizations to prevent or reduce computer crimes. Also here, the same scale was used as in "the beliefs about computer threats and crimes" section. The mean of the responses was used as the measure for this issue.

### 3.4.11 Management and EDP Support.

The management and EDP support was measured by responses to seven questions relevant to management and EDP support to information systems security in Lebanese organizations. Again, the same scale used in "the beliefs about computer threats and crimes" section was applied in this section.

### 3.4.12 Career and Job Attitudes.

This measure was used to judge the respondent satisfaction with their current job position and to indicate their agreement or disagreement with eight statements reflecting their job career and attitudes. The scale used is the same as in the section regarding "the beliefs about computer threats and crimes".

## 3.5 Data Analysis.

The analysis of data was done through the facilities of the Statistical Package for Social Sciences (SPSS). Using this software, a descriptive analysis was conducted to define the followings:

- Describe the situation available in Lebanese computer using organizations concerning computer crimes and security measures they adopt.
- Build a regression equation to study the effect of various factors, such as beliefs about computer threats and crimes, organizations' policies and measures, management and electronic data processing support, and career and job attitudes, upon the computer security level that could be achieved in the organization.

After the presentation of the design and methodology of this research, the variables to be included, and the analysis tools to be utilized, the findings will be displayed in chapter IV and then the assumptions of the study will be evaluated in the light of the hypotheses to be tested.

# CHAPTER IV

## RESEARCH FINDINGS

### 4.1 General overview.

After the methodology, design and tools used for analyzing the data collected for this study, the main purpose of this chapter is to present the findings acquired and to analyze them. It is worth mentioning here that the hypotheses to be tested are listed as follows:

- With the rise of communications networks and microcomputer-based processing, as well as with the general increase in computer literacy, security has become more difficult to manage effectively. Still management does not approach this issue as a serious problem.
- The risk of having computer crimes is highly associated to factors as employee morale and loyalty toward the company, size of the organization, span of control, age, and organizational level .

### 4.2 Profile of Respondents.

The respondents recorded in this study constituted 65.42% response rate, and the size of the sample was 107 computer users. The profession fields of the surveyed end users were Banking , Education, Aviation, and Advertisement. Employees that interact with computer as an essential part of their job, mainly on a regular basis. Due to missing data the questionnaire revealed that 7 cases should be neglected in the

analysis, and this is because some respondents might not have fully understood the questions; Therefore, they gave random responses or skipped questions. Thus, we ended up with 70 significant questionnaires.

With reference to the general characteristics of the 70 respondents, the frequency and percentage method was used here for measuring these characteristics. Results showed that respondents belonged to nine main functional areas: Accounting, Finance, Engineering, General Management, Personnel, Information System, Sales, Marketing and R&D. As it is shown in table VI and chart 4-1, the majority of the respondents belonged to Information System, Accounting, Engineering, and General Management.

**Table VI**
**Functional Area of Respondents.**

| Functional Area | Frequency | Percent | Cumm. % |
|---|---|---|---|
| Accounting | 12 | 17.1 | 17.1 |
| Finance | 4 | 5.7 | 22.9 |
| Engineering | 10 | 14.3 | 37.1 |
| General Management | 12 | 17.1 | 54.3 |
| Personnel | 2 | 2.9 | 57.1 |
| Information System | 13 | 18.6 | 75.7 |
| Sales | 3 | 4.3 | 80.0 |
| Manufacturing/Prod. | 0 | 0.0 | 80.0 |
| Marketing | 5 | 7.1 | 87.1 |
| R&D | 3 | 4.3 | 91.4 |
| Other | 6 | 8.6 | 100 |
| **TOTAL** | 70 | 100.0 | |

Chart 4-1
Functional Area of Respondents

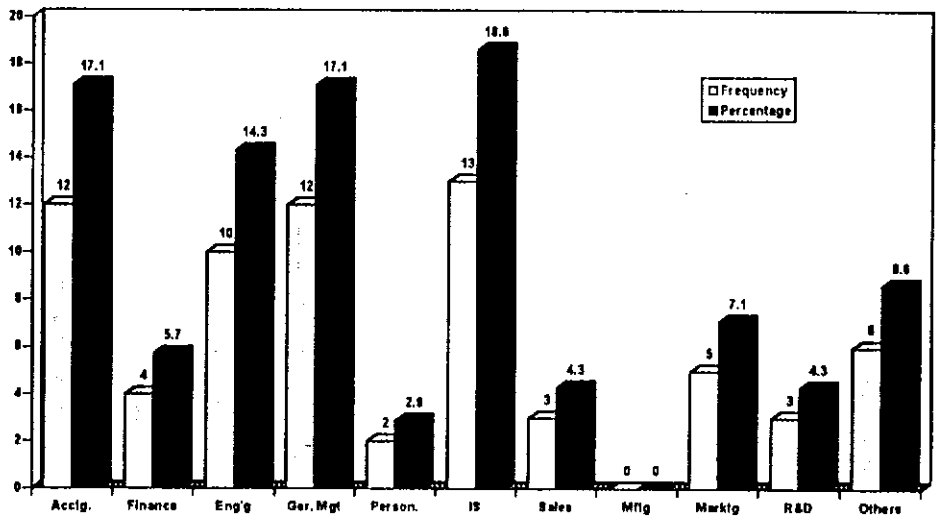
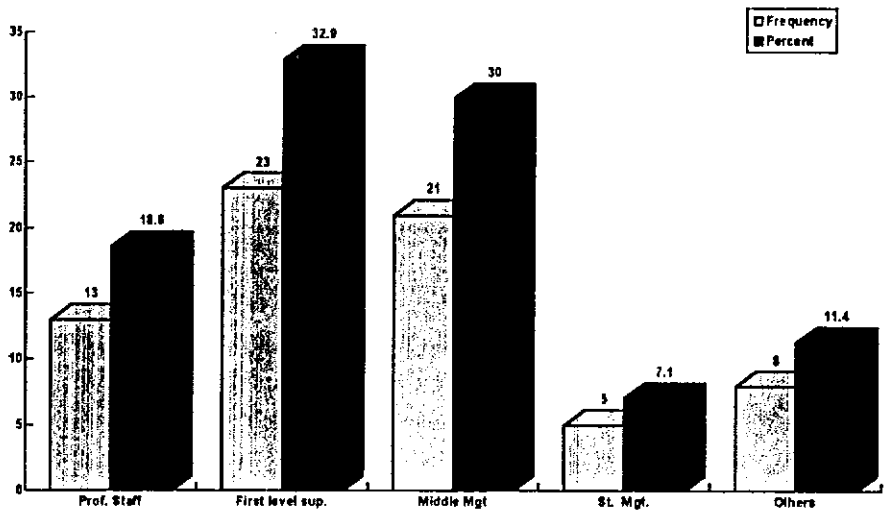



Table VII presents the frequency of the different hierarchy levels that the respondents occupied. There are four main organizational levels: Professional staff, first level supervisor, middle management, and St management. However, as it is displayed in chart 4-2, the majority belonged to first level supervisor and middle management level, or 32.9% and 30% respectively.

**Table VII**
**Hierarchy level of the Respondents.**

| Organization's level | Frequency | Percent | Cumm. % |
|---|---|---|---|
| Prof. Staff | 13 | 18.6 | 18.6 |
| First level Supervisor | 23 | 32.9 | 51.4 |
| Middle Management | 21 | 30.0 | 81.4 |
| St. Management | 5 | 7.1 | 88.6 |
| Other | 8 | 11.4 | 100.0 |
| **TOTAL** | 70 | 100.0 | |

Chart 4-2
Hierarchy level of Respondents

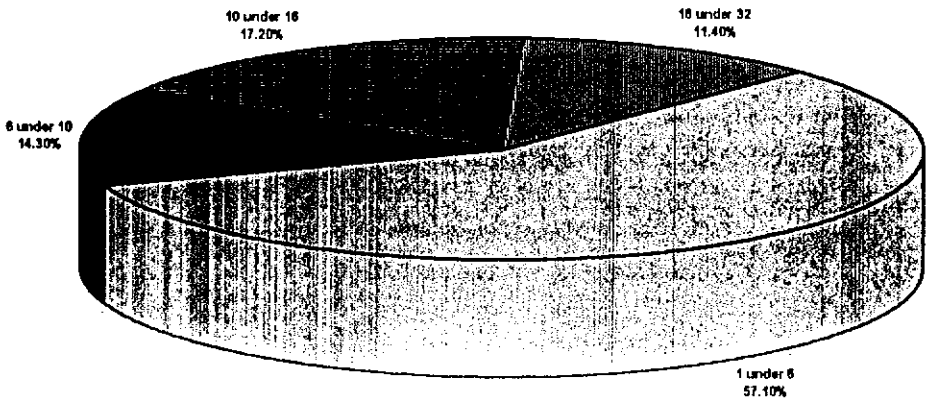



The years spent by the respondents working in his organization ranged from 1 to 32 years, with a majority of employees under 5 years period of work in the same organization, as it is shown in table VIII and chart 4-3.

**Table VIII**
**Years in Organization.**

| Range | Frequency | Percent | Cumm. % |
|---|---|---|---|
| 1-5 | 40 | 57.1 | 57.1 |
| 6-10 | 10 | 14.3 | 71.4 |
| 11-15 | 12 | 17.2 | 88.6 |
| 16-32 | 8 | 11.4 | 100.00 |
| **TOTAL** | 70 | 100.0 | |

Chart 4-3
Years in Organization

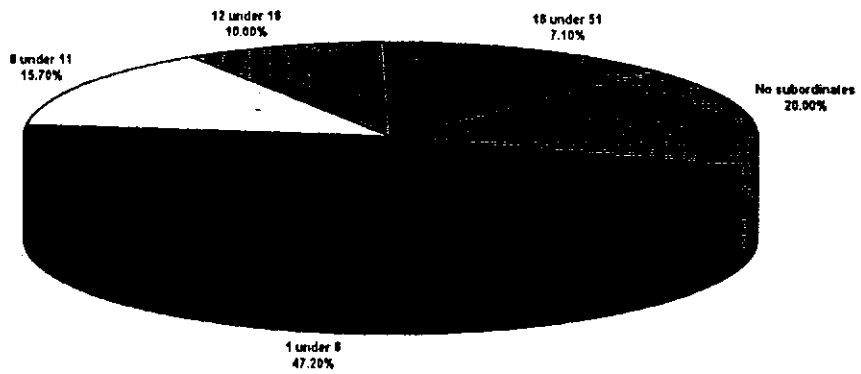



In table IX, there is the number of subordinates reporting to the respondent which ranged from 0 to 50. The majority, which reflected 47.2%, had a number of subordinates that ranged from 1 to 5.

**Table IX**
**Number of Subordinates**

| Range | Frequency | Percent | Cumm. % |
|---|---|---|---|
| 0 | 14 | 20.0 | 20.0 |
| 1-5 | 33 | 47.2 | 67.2 |
| 6-10 | 11 | 15.7 | 82.9 |
| 11-15 | 7 | 10.0 | 92.9 |
| 16-50 | 5 | 7.1 | 100.00 |
| **TOTAL** | 70 | 100.0 | |

Chart 4-4
Number of Subordinates

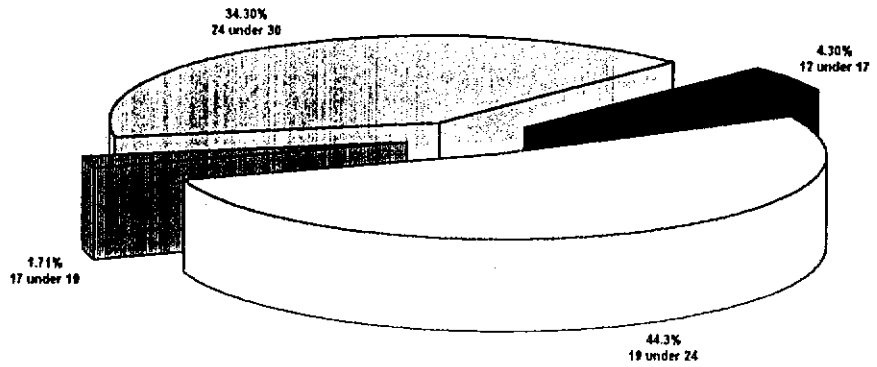



The years of education of the respondents ranged from 12 to 29 years. Examining table X and chart 4-5, one can conclude that the majority of the respondents had more than 19 years of education, in other words, 78.6% of the respondents have minimum high school level.

**Table X**
**Years of Education.**

| Range | Frequency | Percent | Cumm. % |
|---|---|---|---|
| 12-15 | 3 | 4.3 | 4.3 |
| 17-18 | 12 | 17.1 | 21.4 |
| 19-23 | 31 | 44.3 | 65.7 |
| 23-29 | 24 | 34.3 | 100.00 |
| **TOTAL** | 70 | 100.0 | |

Chart 4-5
Years of Education




The age of the respondents ranged between 17 and 61. The average age of the respondents was 32.8 years. The majority of respondents are between 26 and 30 years old. Table XI and chart 4-6 exhibit the above information.

**Table XI**
**Age of Respondents**

| Range | Frequency | Percent | Cumm. % |
|---|---|---|---|
| 17-25 | 14 | 20.0 | 20.0 |
| 26-30 | 27 | 38.6 | 58.6 |
| 31-40 | 14 | 20 | 78.6 |
| 41-61 | 15 | 21.4 | 100.00 |
| **TOTAL** | 70 | 100.0 | |

Chart 4-6
Respondents Age

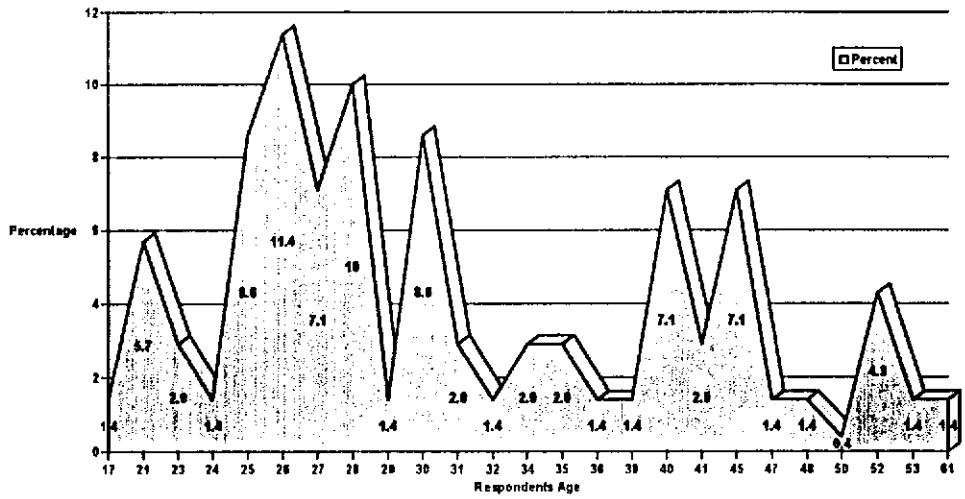



Table XII presents the percentages of respondents' gender. The 67.1% majority of the respondents were males and 32.9% were females.

**Table XII**
**Gender of Respondents**

| Gender | Frequency | Percent | Cumm. % |
|---|---|---|---|
| Male | 47 | 67.1 | 67.1 |
| female | 23 | 32.9 | 100.00 |
| **TOTAL** | 70 | 100.0 | |

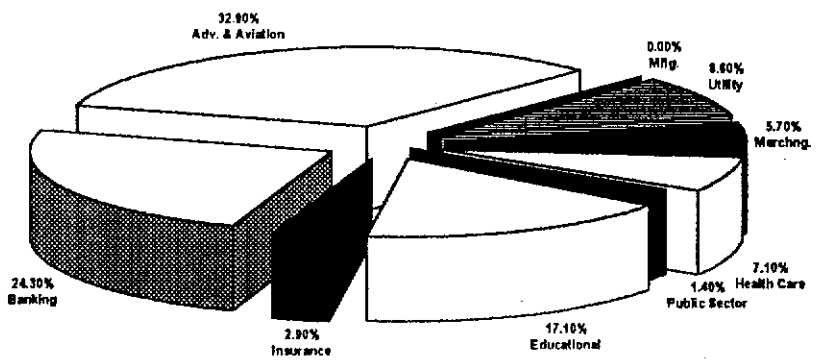
## 4.3 Profile of Organizations.

The characteristics of the organizations to which the respondents belonged were tested by inquiring the primary organization's business and the total number of employees. Organizations' primary business are shown in table XIII and chart 4-7, mainly organization's dealing with Education, Financial services, Advertisements and Aviation.

**Table XIII**
**Primary organization's Business.**

| Organization's Business | Frequency | Percent | Cumm. % |
|---|---|---|---|
| Manufacturing | 0 | 0.0 | 0.0 |
| Utility | 6 | 8.6 | 8.6 |
| Merchandising | 4 | 5.7 | 14.3 |
| Public Sector | 1 | 1.4 | 15.7 |
| Health Care | 5 | 7.1 | 22.9 |
| Insurance | 2 | 2.9 | 25.7 |
| Educational | 12 | 17.1 | 42.9 |
| Financial Services | 17 | 24.3 | 67.1 |
| Other (Adv. Aviation) | 23 | 32.9 | 100.0 |
| **TOTAL** | 70 | 100.0 | |

Chart 4-7
Organizations' Business



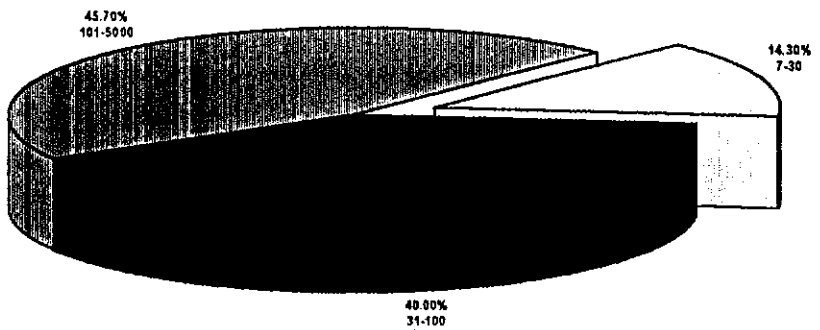

The organizations' size ranged from 7 employees to 5000 employees,. Organizations having below 30 employees could be considered as small organizations, from 31 to 100 as medium, and from 101 to 5000 employees as big and huge organizations. Statistical results

showed that they are mainly medium, big to huge companies. The frequencies of these ranges are listed below in table XIV and chart 4-8.

**Table XIV**
**Number of Employees**

| Range | Frequency | Percent | Cumm. % |
|---|---|---|---|
| 7-30 | 10 | 14.3 | 14.3 |
| 31-100 | 28 | 40.0 | 54.3 |
| 101-5000 | 32 | 45.7 | 100.00 |
| **TOTAL** | 70 | 100.0 | |

Chart 4-8
Organizations Size




It is worth mentioning here that 48.6% of the respondents didn't have any idea about the Data Processing budget set by the organization as an average of the total annual budget, or even if there was any. The range of responses of the knowledgeable respondents was from 1.00% to 30.00%. However, the majority, 25.00% of responses, indicated that this budget was only 3.00% of the total annual budget.

The survey unveiled also that 51.4% of the respondents knew nothing about the security budget as an average of the DP budget. Only 48.6% gave responses that ranged from 1.00% to 30.00%. Also, here the highest percentage of respondents (28.58%) mentioned that the security budget constituted 3.00% as an average percentage of the DP budget.

The above findings raise a very important question which is, why half of the respondents didn't answer both questions. Is it because of unawareness, classified information, or worse both issues are not of an interest to the organization and thus are not included in the annual budget? This is a fact that is widespread among Lebanese organizations. Data processing and Information Systems are installed in organizations gradually and progressively. Whenever a certain necessity or emergency arouse, only then the organization might react to comply with this need or to manage and deal with this crisis. It is infrequent to see an organization planning its IS and preparing budgets for its installation and security. Even when this happens, still security is assigned low value in the budget or is even disregarded.

## 4.4 Systems Used and Usage.

System used is analyzed using two questions' subsections. Both results are listed in table XV. The majority of the systems were connected to other computers or networks, most of the respondent did not own the computer, and the systems were mainly PCs.

A very important fact to mention here is that, a very high percentage or almost all respondents had free access to the system. This element is one of the main factors that affects negatively security of Information Systems. When nearly all employees have free access to the system and the data, responsibility can not be assigned in case data was destructed or deleted. Moreover, any employee can access files and information that he/she is not supposed to see, he/she might also manipulate or steal the data for his/her personnal benefits. This risk increases when computers are connected via networks since master files and organization programs might be jeopardised.

**Table XV**
**System Used.**

| Characteristics | Frequency | Percent | Cumm. % |
|---|---|---|---|
| -Stand alone | 22 | 31.4 | 31.4 |
| -Connected to other computers or networks | 48 | 68.6 | 100.0 |
| -The respondent own computer | 22 | 31.4 | 31.4 |
| -The respondent does not own computer | 48 | 68.6 | 100.0 |
| -The respondent has free access | 69 | 98.6 | 98.6 |
| -The respondent does not have free access | 1 | 1.4 | 100.0 |
| -System is a non PC (mainframe/minicomp.) | 27 | 38.6 | 38.6 |
| -System is a PC | 43 | 61.4 | 100.0 |

System usage was examined by testing three areas which are shown in table XVI and chart 4-9 and chart 4-10. Mainly, a big portion of

respondents had used the system, on an average weekly day, from 4 to 8 hours. Furthermore, on an average, about 70% a high percentage of respondents were exposed to the system operation more than 20 days per month. The majority of respondents had been using this system for less than 5 years, the mean was calculated to be 5.314 years.

**Table XVI**
**System Usage.**

| Characteristics | Range | Freq. | % | Cum. % |
|---|---|---|---|---|
| - On an average weekly day, the hours of system usage by the respondent | 0 under 2 | 2 | 2.9 | 2.9 |
| | 2 under 4 | 19 | 27.1 | 30.0 |
| | 4 under 6 | 23 | 32.9 | 62.9 |
| | 6 under 8 | 26 | 37.1 | 100.0 |
| - On an average the respondent daily system usage during a month. | 0 under 5 | 1 | 1.4 | 1.4 |
| | 5 under 10 | 3 | 4.3 | 5.7 |
| | 10 under 15 | 12 | 17.1 | 22.9 |
| | 15 under 20 | 5 | 7.1 | 30.0 |
| | 20 under 25 | 24 | 34.3 | 64.3 |
| | 25 under 30 | 25 | 35.7 | 100.0 |
| - Years of system usage by the respondent. | 1 under 5 | 39 | 55.7 | 55.7 |
| | 5 under 10 | 18 | 25.7 | 81.4 |
| | 10 under 15 | 13 | 18.6 | 100.0 |

Chart 4-9
Average Hours/Day

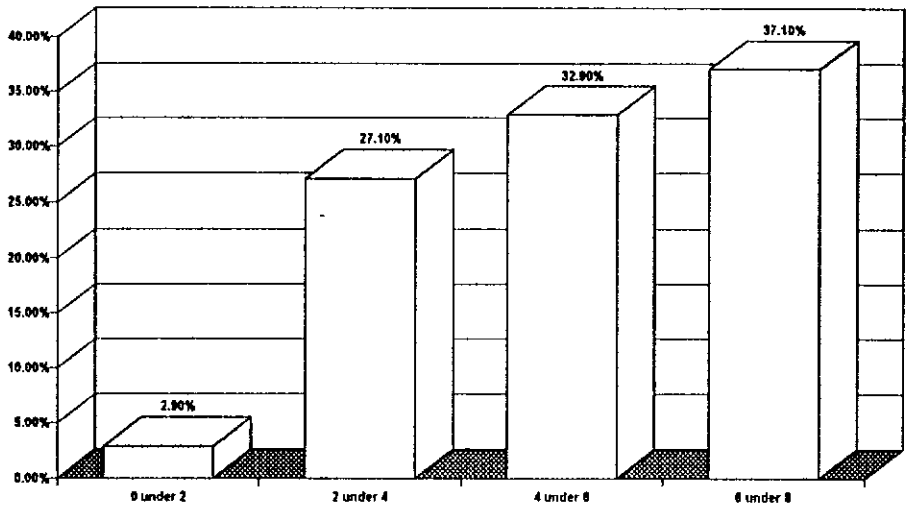
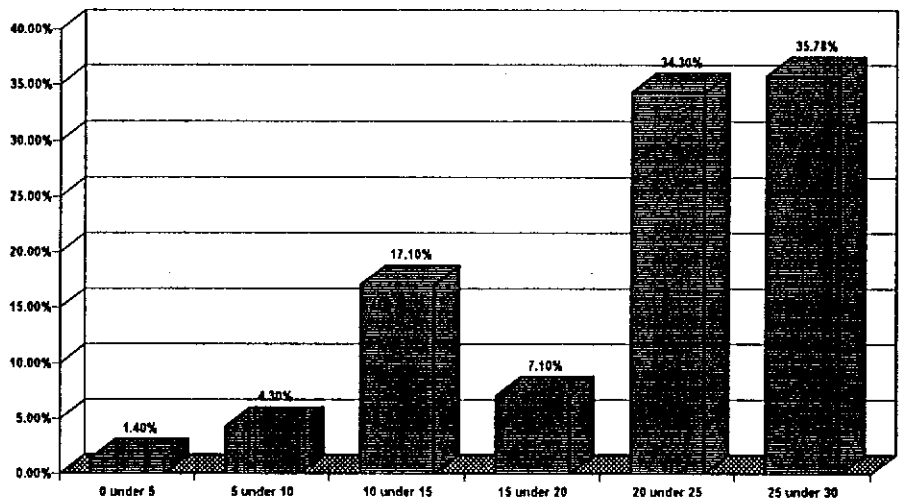



Chart 4-10
Average Days/Month




## 4.5 Computer Training.

The level of the respondents computer training was measured by the extent of this training from four major sources. The majority of respondents (80.00%) revealed that they had acquired their training

extensively through self study; 41.40% via general courses at college or university; 32.90% in house company courses, and finally, 22.90% through training provided by outside consultants. Thus, an average of 4.157, 3.171, 2.786, and 2.543 respectively. In this section, one can notice the absence of 'in house company courses and outside consultants' which constitutes a threat to security since most of the employees are augmenting their computer knowledge and solving their computer problems by trial and error. This, in turn, might endanger data, software and hardware.

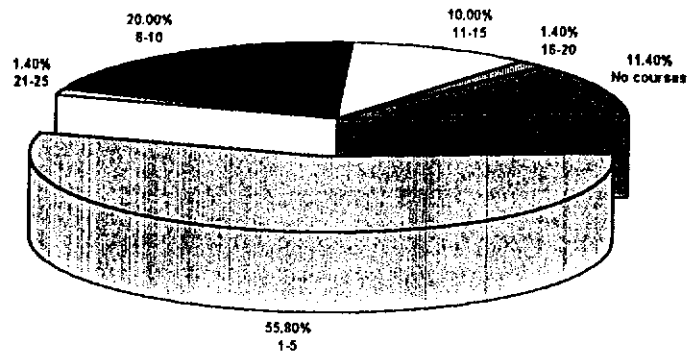
## 4.6 Computer Knowledge and Experience.

With reference to computer courses taken by the respondents, the numbers ranged from 0 to 25 . Table XVII and chart 4-11 exhibit the findings. The majority had taken less than 6 courses, and a good portion, 20%, had taken from 6 to 10 courses. Mean was computed to be 5.329.

**Table XVII**
**Courses Taken in Computer**

| Range | Frequency | Percent | Cumm. % |
|---|---|---|---|
| 0 | 8 | 11.4 | 11.4 |
| 1-5 | 39 | 55.8 | 67.2 |
| 6-10 | 14 | 20.0 | 87.2 |
| 11-15 | 7 | 10.0 | 97.2 |
| 16-20 | 1 | 1.4 | 98.6 |
| 21-25 | 1 | 1.4 | 100.00 |
| **TOTAL** | 70 | 100.0 | |
| **Mean =5.329** | | | |

Chart 4-11
Courses taken in Computers

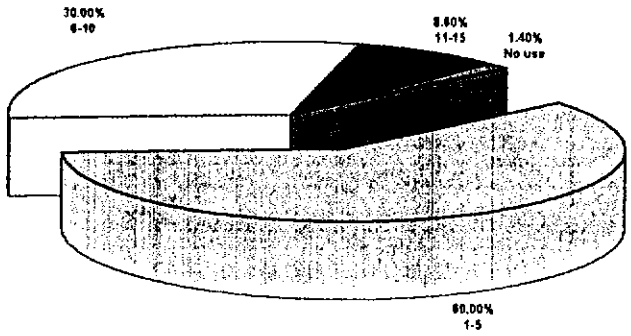



For the period spent by the respondents on using a PC , statistical results showed a range from 0 to 14 years, with 60% range of 1 to 5 years of PC use and an average of 5.300 years. Again, table XVIII and chart 4-12 display the above findings.

**Table XVIII**
**Years of PC Use**

| Range | Frequency | Percent | Cumm. % |
|---|---|---|---|
| 0 | 1 | 1.4 | 1.4 |
| 1-5 | 42 | 60.0 | 61.4 |
| 6-10 | 21 | 30.0 | 91.4 |
| 11-15 | 6 | 8.6 | 100.00 |
| **TOTAL** | 70 | 100.0 | |
| **Mean =5.300** | | | |

Chart 4-12
Years of PC Use

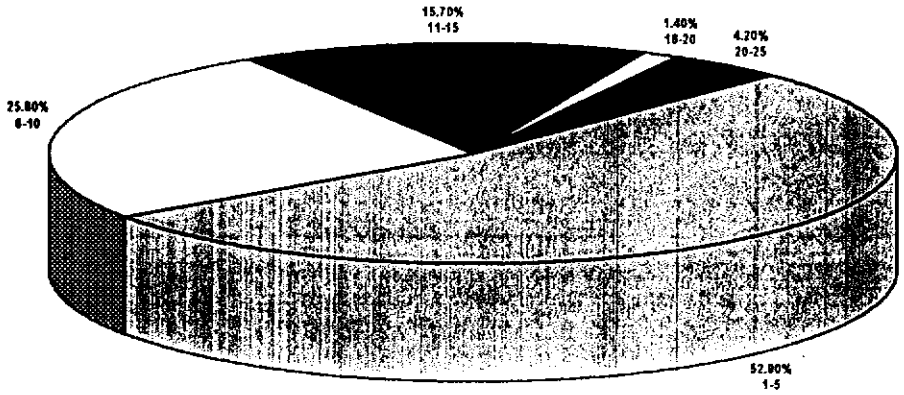



The period spent on using computers in general by the respondents, ranged from 1 to 23. Also here, the highest percentage was for the period range of 1 to 5 years, and with an average of 7.114 years. Table XIX and chart 4-13 manifest the above results.

**Table XIX**
**Years of Computers Use**

| Range | Frequency | Percent | Cumm. % |
|---|---|---|---|
| 1-5 | 37 | 52.9 | 52.9 |
| 6-10 | 18 | 25.8 | 78.7 |
| 11-15 | 11 | 15.7 | 94.4 |
| 16-20 | 1 | 1.4 | 95.8 |
| 20-25 | 3 | 4.2 | 100.00 |
| **TOTAL** | 70 | 100.0 | |
| **Mean =7.114** | | | |

Chart 4-13
Years of Computers Use

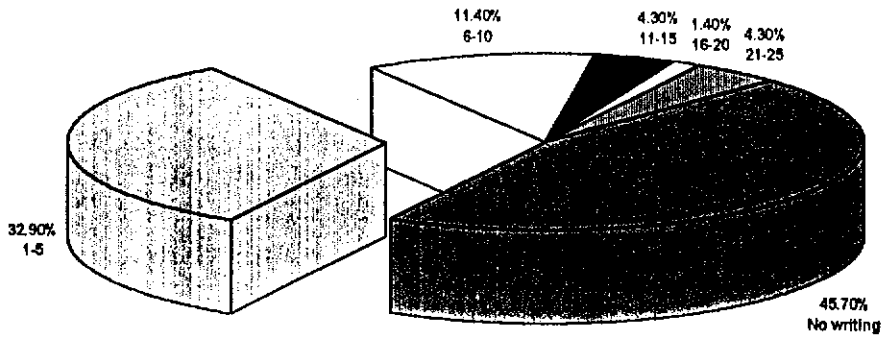



The period spent by the respondent in writing programs by using computer languages ranged from 0 to 23. In table XX and chart 4-14, one can see that only half of the respondents wrote programs in computer language. The majority of these respondents did not have more than 5 years of experience and actual practice in programming. The mean was 3.529 years.

**Table XX**
**Years Writing in Computer Language.**

| Range | Frequency | Percent | Cumm. % |
|---|---|---|---|
| 0 | 32 | 45.7 | 45.7 |
| 1-5 | 23 | 32.9 | 78.6 |
| 6-10 | 8 | 11.4 | 90.0 |
| 11-15 | 3 | 4.3 | 94.3 |
| 16-20 | 1 | 1.4 | 95.7 |
| 20-25 | 3 | 4.3 | 100.00 |
| **TOTAL** | 70 | 100.0 | |
| **Mean =3.529** | | | |

**Chart 4-14**
**Years Writing in Computer Language**




## 4.7 Information System Management.

In ranking the top 3 issues for Information System Management according to their importance and from 10 issue listed, the survey exposed the following final ranking shown in table XXI, XXII, XXIII. The ranking as number one within the ten issues was based on the percentage of vote. The same was applied for ranking the second and the third issue.

One can conclude that "Management and facilitation of end user computing" issue got the highest percentage in ranking as number one and number two issue. "Effective use of the organization's data resources" also had high percentage of votes. It was ranked first as being the number one and number three top issue.

"Improving security measures for information system", which is of real interest in this ranking, was ranked third as number one issue, sixth as number two, and finally second as number three issue.

**Table XXI**
**Number One Issue in ISM**

| % | Rank | Issue Description |
|---|---|---|
| 17.1 | 1 | Management and facilitation of end user computing. |
| 17.1 | 1 | Effective use of the organization's data resources. |
| 14.3 | 3 | Improving security measures for information systems. |
| 12.9 | 4 | Improved information system planning. |
| 8.6 | 5 | Integration of data processing, office automation, and telecommunications. |
| 8.6 | 5 | Development and implementation of decision support systems. |
| 7.1 | 7 | Alignment of the IS organization with that of the enterprise. |
| 5.7 | 8 | Facilitation of organizational learning and use of information system technologies. |
| 4.3 | 9 | Improved software development and quality. |
| 4.3 | 9 | Specification, recruitment, and development of IS human resources. |

**Table XXII**
**Number Two Issue in ISM**

| % | Rank | Issue Description |
|---|---|---|
| 21.4 | 1 | Management and facilitation of end user computing. |
| 14.3 | 2 | Integration of data processing, office automation, and telecommunications. |
| 14.3 | 2 | Facilitation of organizational learning and use of information system technologies. |
| 12.9 | 4 | Effective use of the organization's data resources. |
| 8.6 | 5 | Improved software development and quality. |
| 7.1 | 6 | Improving security measures for information systems. |
| 7.1 | 6 | Alignment of the IS organization with that of the enterprise. |
| 7.1 | 6 | Development and implementation of decision support systems. |
| 5.7 | 9 | Improved information system planning. |
| 2.9 | 10 | Specification, recruitment, and development of IS human resources. |

**Table XXIII**
**Number Three Issue in ISM**

| % | Rank | Issue Description |
|---|---|---|
| 20.0 | 1 | Effective use of the organization's data resources. |
| 14.3 | 2 | Improving security measures for information systems. |
| 14.3 | 2 | Development and implementation of decision support systems. |
| 14.3 | 2 | Integration of data processing, office automation, and telecommunications. |
| 12.9 | 5 | Facilitation of organizational learning and use of information system technologies. |
| 10.0 | 6 | Improved information system planning. |
| 8.6 | 7 | Improved software development and quality. |
| 2.9 | 8 | Management and facilitation of end user computing. |
| 1.4 | 9 | Specification, recruitment, and development of IS human resources. |
| 0.0 | 10 | Alignment of the IS organization with that of the enterprise. |

## 4.8 Threats to Information System Security.

In ranking the top 3 threats, from 12 threats listed, on Information System Management according to their effects on computer security, the same method used for ranking the most important issues for Information System Management was used here. The final ranking is listed in tables XXIV, XXV, XXVI respectively.

Statistical results indicated that accidental and intentional entry of 'bad' data by employees were the most dangerous to the organization's information system. That's why they were ranked as number one threat. "Accidental destruction of data by employees" was ranked first as the top number two threat to ISS. Ranked first as the top three threat was the risk of "Natural disaster, loss of power, communications".

No matter what the threat was or its source, the conclusion that one can deduce by reviewing these three tables is that "Employee's Behavior ", according to the respondents, was the most important and relevant factor related to possible threat to the organization's ISS. Whether it was intentional or involuntary, employee's conduct was considered to be the major source of threat to the ISS.

**Table XXIV**
**Number One Threat to ISS.**

| % | Rank | Threat Description |
|---|---|---|
| 15.7 | 1 | Accidental entry of 'bad' data by employees. |
| 15.7 | 1 | Intentional entry of 'bad' data by employees. |
| 14.3 | 3 | Entry into system of computer viruses. |
| 12.9 | 4 | Accidental destruction of data by employees. |
| 11.4 | 5 | Poor control over manual handling of I/O. |
| 7.1 | 6 | Intentional destruction of data by employees. |
| 5.7 | 7 | Weak, ineffective, inadequate physical control. |
| 4.3 | 8 | Unauthorized access to data/system by employees. |
| 4.3 | 8 | Access to data/system by outsiders(hackers). |
| 4.3 | 8 | Natural disaster, loss of power, communications. |
| 2.9 | 11 | Inadequate control over media (disks, tapes). |
| 2.9 | 11 | Access to data/system by outsiders(competitors). |

**Table XXV**
**Number Two Threat to ISS.**

| % | Rank | Threat Description |
|---|---|---|
| 17.1 | 1 | Accidental destruction of data by employees. |
| 12.9 | 2 | Unauthorized access to data/system by employees. |
| 11.4 | 3 | Intentional destruction of data by employees. |
| 10.0 | 4 | Poor control over manual handling of I/O. |
| 8.6 | 5 | Accidental entry of 'bad' data by employees. |
| 8.6 | 5 | Inadequate control over media (disks, tapes). |
| 8.6 | 5 | Access to data/system by outsiders(hackers). |
| 7.1 | 8 | Intentional entry of 'bad' data by employees. |
| 7.1 | 8 | Entry into system of computer viruses. |
| 5.7 | 10 | Natural disaster, loss of power, communications. |
| 2.9 | 11 | Weak, ineffective, inadequate physical control. |
| 0.0 | 12 | Access to data/system by outsiders(competitors). |

**Table XXVI**
**Number Three Threat to ISS.**

| % | Rank | Threat Description |
|---|---|---|
| 27.1 | 1 | Natural disaster, loss of power, communications. |
| 12.9 | 2 | Accidental entry of 'bad' data by employees. |
| 11.4 | 3 | Entry into system of computer viruses. |
| 8.6 | 4 | Unauthorized access to data/system by employees. |
| 7.1 | 5 | Poor control over manual handling of I/O. |
| 7.1 | 5 | Accidental destruction of data by employees. |
| 5.7 | 7 | Intentional destruction of data by employees. |
| 5.7 | 7 | Access to data/system by outsiders(hackers). |
| 5.7 | 7 | Weak, ineffective, inadequate physical control. |
| 4.3 | 10 | Intentional entry of 'bad' data by employees. |
| 4.3 | 10 | Inadequate control over media (disks, tapes). |
| 0.0 | 12 | Access to data/system by outsiders(competitors). |

In examining the respondents assessment of the risk level of computer disruption in three different environments, the survey showed that 42.9% of the respondents saw moderate risk in Microcomputer, 40% as low or very low risk, and only 17.1% assumed there was high or very high risk. The mean was calculated to be 2.657. For networks, on the other hand, 35.7% of respondents believed that the risk was moderate, 24.3% as low or very low risk, and 40.0% presumed that there was high or very high risk. Hence, an average of 3.200. Mainframes have low or very low risk of disruption, according to 48.6% of the respondents, and 35.7% saw that the risk was moderate; However, only 15.7% assumed that there was high or very high risk. Consequently, a mean of 2.571.

In summary, The overall risk of computer disruption was moderate according to 51.4% of the respondents, 30.0% judged low or

very low risk, and the remaining 18.6% calculated high or very high risk, with a mean of 2.886. Nevertheless, it is very important to note here the high percentage of respondents (40.0%) that evaluated high or very high risk of computer disruption in Networks in comparison to the other two environments.

## 4.9 Computer Viruses Relative to other Threats.

The findings of this section demonstrated the importance of IS security and the level of awareness and its application within Lebanese organizations. The survey indicated that 65.7% of the respondents had witnessed incidents of computer disruption due to the intrusion of computer viruses. one already knows that there is not 100% secure system, still the above percentage is very high and can not be tolerated.

Even though only 15.8% of these organizations have high and very high risk of computer disruption, this percentage should not be overlooked if one knows what a virus can exert. Moreover, having 38.6% of the respondents assessing moderate risk is not something to be disregarded. Sometimes one file altered, modified or deleted might cause tremendous and vital disturbance in the whole organization.

In the last section of this part, respondents were asked to judge their organization concern and interest about the issue of computer viruses, again 32.8% of the responses agreed or strongly agreed that this is not a major concern in their organization. Additionally, 38.6% of

respondents were neutral or even didn't know if this issue was of any concern to management.

## 4.10 Computer Viruses Prevention.

Respondents suggestions, regarding measures that could be followed to prevent infection by computer viruses, showed that "Backup procedures schedules" action is presumed to be the most efficient way for viruses prevention. Responses mean for this aspect was 1.771 based on a Likert type scale from (1), "Strongly Agree", to (5), "Strongly Disagree". Then, there are "The use of passwords" and "Use of virus scanning software" as two other important actions, while "Auto terminal/account logoff earned the lowest number of votes. The average mean for all 14 aspects was calculated to be 2.399 which means almost an agreement with the efficiency of the aspects listed as methods for virus anticipation. Table XXV will list the 14 actions, according to their efficiency to prevent viruses intrusion, based on the mean of the responses.

**Table XXV**
**Ranking of Preventive Measures Against Computer Viruses.**

| Mean | Rank | Issue Description |
|---|---|---|
| 1.771 | 1 | Backup procedures schedules |
| 1.814 | 2 | The use of passwords |
| 1.900 | 3 | Use of virus scanning software |
| 1.914 | 4 | Employee education |
| 2.129 | 5 | Consistent security policies |
| 2.286 | 6 | Company-provided software only |
| 2.371 | 7 | Control of workstations |
| 2.529 | 8 | Monitor computer user usage |
| 2.543 | 9 | Audit procedures strengthened |
| 2.714 | 10 | Reporting violations encouraged |
| 2.829 | 11 | Publish formal standards |
| 2.871 | 12 | No outside connections |
| 2.914 | 13 | Ethics training |
| 3.000 | 14 | Auto terminal/account logoff |
| | | **Mean = 2.399** |

When it comes to measure the extent to which each application was applied in the respondent's organization, it was found out that the same top three methods suggested by the respondents in the above section were also the most practiced in the respondent's organization "Backup procedures schedules" issue came in the first place with a mean of 3.371 based on a a Likert type scale from (1), "Not at All", to (5), "To a Great Extent". "The use of passwords" and "Use of virus scanning software" actions ranked next; Nevertheless, "Ethics training" earned a very low number of votes. The average mean of all the 14 issues was 2.732 which roughly reflect responses ranging between moderate and low application level of these preventive actions by organizations. Table XXVI exhibits the above results.

**Table XXVI**
**Ranking of Applied Preventive Measures Against Computer Viruses.**

| Mean | Rank | Issue Description |
|---|---|---|
| 3.371 | 1 | Backup procedures schedules |
| 3.186 | 2 | The use of passwords |
| 2.886 | 3 | Use of virus scanning software |
| 2.871 | 4 | Employee education |
| 2.814 | 5 | company-provided software only |
| 2.743 | 6 | Audit procedures strengthened |
| 2.700 | 7 | Consistent security policies |
| 2.686 | 8 | Monitor computer user usage |
| 2.671 | 9 | No outside connections |
| 2.629 | 10 | Control of workstations |
| 2.629 | 10 | Auto terminal/account logoff |
| 2.571 | 12 | Publish formal standards |
| 2.514 | 13 | Reporting violations encouraged |
| 1.971 | 14 | Ethics training |
| | | **Mean = 2.732** |

## 4.11 Regression Analysis.

To check the validity of the hypothesis stated to integrate the factors that are most likely to be associated with maintaining a high level of computer security in organizations, the regression analysis was used to build regression equations that could depict the potential relationships between dependent variables and independent variables. A dependent variable is the variable whose variation is likely to be explained, and an independent variable is a variable used to explain the variation in the dependent variable. The intention, here, was to build several regression equations, taken career and job attitudes, Management and EDP support, beliefs about computer threats and crimes, preventive procedures followed, and suggested and applied viruses prevention methods as dependent variables and the other variables as independent variables.

### 4.11.1 Building a Regression Equation with Career and Job Attitudes being the Dependent Variable:

The first step in developing the regression model was to examine the relationship between each independent variable and the dependent variables, and between each independent variable with other independent variables. The dependent variable was career and job attitudes (ZCA), and the independent variables selected were level in the organization's hierarchy, years in organization, number of subordinates, educational level, age, gender, total number of employees in the organization, data processing budget, and the size of the IS security budget. The resulting correlation matrix is shown in table XXVII.

**Table XXVII**
**Correlation Matrix between Career and Job Attitudes and Independent Variables**

| □ | ZCA | Z2 | X4 | X5 | X6 | X7 | X8 | X9 | X10 | X11 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | □ |
| ZCA | 1.000 | .245 | .728 | .168 | .419 | .729 | .041 | .464 | .120 | .120 |
| | | .247 | .009 | .321 | .114 | .008 | .445 | .089 | .371 | .371 |
| Z2 | .245 | 1.000 | .478 | -.085 | .293 | .594 | .333 | .749 | -.098 | -.098 |
| | .247 | | .081 | .408 | .506 | .035 | .173 | .006 | .394 | .394 |
| X4 | .728 | .478 | 1.00 | .625 | .318 | .961 | .232 | .433 | .488 | .488 |
| | .009 | .081 | 0 | .027 | .185 | .000 | .260 | .106 | .076 | .076 |
| X5 | .168 | -.085 | .625 | 1.00 | -.165 | .502 | .282 | -.059 | .742 | .742 |
| | .321 | .408 | .027 | 0 | .324 | .069 | .215 | .435 | .007 | .007 |
| X6 | .419 | .293 | .318 | -.165 | 1.000 | .357 | .000 | .181 | .048 | .048 |
| | .114 | .506 | .185 | .324 | | .156 | .500 | .308 | .448 | .448 |
| X7 | .729 | .594 | .961 | .502 | .357 | 1.00 | .279 | .619 | .409 | .409 |
| | .008 | .035 | .000 | .069 | .156 | 0 | .217 | .028 | .120 | .120 |
| X8 | .041 | .333 | .232 | .282 | .000 | .279 | 1.000 | .134 | .163 | .163 |
| | .445 | .173 | .260 | .215 | .500 | .217 | | .356 | .327 | .327 |
| X9 | .464 | .749 | .433 | -.059 | .181 | .619 | .134 | 1.00 | -.026 | -.026 |
| | .089 | .006 | .106 | .435 | .308 | .028 | .356 | 0 | .471 | .471 |
| X10 | .120 | -.098 | .488 | .742 | .048 | .409 | .163 | -.026 | 1.00 | 1.000 |
| | .371 | .394 | .076 | .007 | .448 | .120 | .327 | .471 | 0 | .000 |
| X11 | .120 | -.098 | .488 | .742 | .048 | .409 | .163 | -.026 | 1.00 | 1.000 |
| | .371 | .394 | .076 | .007 | .448 | .120 | .327 | .471 | 0 | |
| | | | | | | | | | .000 | |

As could be noticed, there is a high correlation coefficient between the variables years in the organization and age, and the dependent variable career and job attitudes (ZCA). The value of the correlation coefficient could also assist in assigning a relative importance to each independent factor in defining or explaining the variation in the dependent variable. By reading the coefficients of correlation between ZCA and the independent variables, such an explanation can be determined. The table shows that X7 (age) has the highest correlation coefficient among all the independent variables with ZCA, followed by years in organization, total number of employees in the organization, and so on. Thus, the independent variables could be ranked in the order of their importance as potential predictors of ZCA. Also, a stepwise regression analysis was used to build the regression equation through a forward selection of variables.

As expected, the first independent variable entered to the regression equation was age. Table XXVIII shows the results of the first regression output at a significance level of 0.05 $R^2$, the coefficient of determination shows how much the variations in the dependent variable could be explained by the independent variables included.

**Table XXVIII**
**Regression Output-Dependent Variable=ZCA**

Variable (s) Entered on Step Number
1.. X7

| | |
|---|---|
| Multiple R | .72890 |
| R Square | .53129 |
| Adjusted R Square | .47271 |
| Standard Error | .31209 |

Analysis of Variance

| | DF | Sum of Squares | Mean Square |
|---|---|---|---|
| Regression | 1 | .88328 | .88328 |
| Residual | 8 | .77922 | .09740 |

F= 9.06825 Signif F= .0168

In this output, $R^2$=0.5313; i.e., 53.13%, which means that about 53% of the variations in the respondents' career and job attitudes could be explained by the "age" factor. No other variables entered into the equation. The coefficient of the independent variable is the beta value shown in table XXIX. Beta shows the value of change in the dependent variable due to one standard deviation change in a given in dependent variable, holding other variables constant. As a result, the regression equation is:

$$ZCA=1.668 + 0.728X7$$

$$(0.0074) \quad (0.0168)$$

$$R^2= 0.5313= 53.13\%$$

**Table XXIX**
**Beta Coefficients and the Test for**
**Significance of the Independent Variable**

| Variable | Beta | T | Sig. T |
|---|---|---|---|
| X7 (Age) | 0.728899 | 3.011 | 0.0168 |
| (constant) | 1.668467 | 3.555 | 0.074 |

A- The Significance of the Overall Regression Model.

The R square (multiple coefficient of determination) is given in the output run generated by the computer as 0.5313. Therefore, almost 53% of the variation in career and job attitudes can be explained by the only one independent variable included in the regression model, namely age.

An analysis of variance F test can be used to test the overall significance of the regression model. To test the model's significance, the critical F value is compared to the level of significance used (0.05). Since F critical (0.0168) < level of significance (0.05), the regression model is considered significant.

B- The Significance of the Individual Variable.

The significance of the independent variable included can be tested through using a t- test. The calculated t- value is provided in table XXIX and the significant t is put in parentheses under the relevant independent variable in the equation. The significance is achieved if the significant t is less than the level of significance used (0.05). The test is:

For age (X7): Significant T= 0.0168.

Since 0.0168 < 0.05

Then X7 is a significant variable.

C- Interpretation of the Equation.

The resulting regression equation could be easily interpreted. As for age (X7), the value of Beta, 0.728899, indicates that for each added value in age, career and job attitudes would directly vary by the value of 0.728899. Moreover, the positive sign of the beta coefficient of this variable indicates that the linear relationship between age and career and job attitudes is positive. The higher the age of the employee, the higher would be the degree of the career and job attitude of the employee in the organization. This could be attributed to the possibility that the higher the age of the employee, the more one would be expected to have spent time in the job one is performing and the career one is holding, and thus the more positive attitudes towards the job. Studying job attitudes and knowing the factors affecting it is a growing concern among organizations, since it is believed that if employees are satisfied with their jobs and with the way management is treating them, then this will lead them to accept and be satisfied with new information systems[35] . A Satisfied employee will do his/her best to protect and maintain the system he is using. This of course, will lead to better handling of information systems and improved security for these systems.

---

35 M. Lynn Markus and Neils Andersen, "Power Over Users: Its Exercise by System Professional", Communication of the ACM, Vol. 30, No. 6, June 1987, p.p. 498-504.

### 4.11.2 Building a Regression Equation with Management and EDP Support being the Dependent Variable:

The same procedure followed with job and career attitudes would be followed here to derive a regression equation that could help in explaining variations in the dependent variable Management and EDP support (ZB). The independent variables selected were the same ones selected for the previous model. The correlation matrix presented in table XXX shows the relationship between the dependent variable Management and EDP support and each of the independent variables, also the relationship between each independent variable and the other independent variables.

**Table XXX**
**Correlation Matrix between Management and EDP Support and Independent Variables**

| □ | ZB | Z2 | X4 | X5 | X6 | X7 | X8 | X9 | X10 | X11 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | □ |
| ZB | 1.000 | -.391 | .430 | .660 | -.327 | .379 | .056 | .015 | .626 | .626 |
| | | .132 | .108 | .019 | .178 | .140 | .439 | .484 | .026 | .026 |
| Z2 | -.391 | 1.000 | .478 | -.085 | .293 | .594 | .333 | .749 | -.098 | -.098 |
| | .132 | | .081 | .408 | .206 | .035 | .173 | .006 | .394 | .394 |
| X4 | .430 | .478 | 1.00 | .625 | .318 | .961 | .232 | .433 | .488 | .488 |
| | .108 | .081 | 0 | .027 | .185 | .000 | .260 | .106 | .076 | .076 |
| X5 | .660 | -.085 | .625 | 1.00 | -.165 | .502 | .282 | -.059 | .742 | .742 |
| | .019 | .408 | .027 | 0 | .324 | .069 | .215 | .435 | .007 | .007 |
| X6 | -.327 | .293 | .318 | -.165 | 1.000 | .357 | .000 | .181 | .048 | .048 |
| | .178 | .206 | .185 | .324 | | .156 | .500 | .308 | .448 | .448 |
| X7 | .379 | .594 | .961 | .502 | .357 | 1.00 | .279 | .619 | .409 | .409 |
| | .140 | .035 | .000 | .069 | .156 | 0 | .217 | .028 | .120 | .120 |
| X8 | .056 | .333 | .232 | .282 | .000 | .279 | 1.000 | .134 | .163 | .163 |
| | .439 | .173 | .260 | .215 | .500 | .217 | | .356 | .327 | .327 |
| X9 | .015 | .749 | .433 | -.059 | .181 | .619 | .134 | 1.00 | -.026 | -.026 |
| | .484 | .006 | .106 | .435 | .308 | .028 | .356 | 0 | .471 | .471 |
| X10 | .626 | -.098 | .488 | .742 | .048 | .409 | .163 | -.026 | 1.00 | 1.000 |
| | .026 | .394 | .076 | .007 | .448 | .120 | .327 | .471 | 0 | .000 |
| X11 | .626 | -.098 | .488 | .742 | .048 | .409 | .163 | -.026 | 1.00 | 1.000 |
| | .026 | .394 | .076 | .007 | .448 | .120 | .327 | .471 | 0 | |
| | | | | | | | | | .000 | |

The table shows that X5, the number of subordinates reporting to the manager, is the most important factor in determining Management and EDP support since it has the strongest positive relationship with ZB. This is followed by X10 (data processing budget), X11 (size of the IS security budget), and so on.

Here also a stepwise regression method was used to examine the forward selection of variables, and the extent of each user's influence on ZB. The only variable that was included in the equation was the number of subordinates reporting to the manager. The regression output was as follows:

**Table XXXI**
**Regression Output-Dependent Variable=ZB**

Variable (s) Entered on Step Number
1.. X5

| | |
|---|---|
| Multiple R | .66041 |
| R Square | .43614 |
| Adjusted R Square | .36565 |
| Standard Error | 3.00832 |

Analysis of Variance

| | DF | Sum of Squares | Mean Square |
|---|---|---|---|
| Regression | 1 | 56.00000 | 56.00000 |
| Residual | 8 | 72.40000 | 9.05000 |

F= 6.18785 Signif F= .0377

The coefficient of the independent variable X5 is the beta value listed in table XXXII. As a result, the regression equation that could be built for predicting Management and EDP support is:

$$ZB=15.6 + 0.66041X5$$

$$(0.0000) \quad (0.0377)$$

$$R^2= 0.43614= 43.6\%$$

**Table XXXII**
**Beta Coefficients and the Test for Significance of the Independent Variable**

| Variable | Beta | T | Sig. T |
|---|---|---|---|
| X5 | 0.660407 | 2.488 | 0.0377 |
| (constant) | 15.600 | 12.524 | 0.000 |

A- The Significance of the Overall Regression Model.

The R square (multiple coefficient of determination) is given in the computer printout as 0.436. This means that 44% of the variation in Management and EDP support could be explained by the number of subordinates reporting to the manager. Moreover, to test the model's significance, the critical F value, 0.0377 is compared to the significance level 0.05. Since critical F value < significance level, the regression model could be considered significant.

B- The Significance of the Individual Variable.

The significance of the independent variable could be tested using the t- test. The significant t values are presented in table XXXII and put in parentheses under the relevant independent variable. Taking into consideration that the significance of each variable is achieved if the sig. t is less than the significance level, then it could be concluded that the variable X5 included in the regression model is significant in explaining the variation of Management and EDP support.

C- Interpretation of the Equation.

The interpretation of the regression equation of Management and EDP support is straightforward. As for the beta coefficient of X5, it is 0.66041, indicating that if the number of subordinates changes by one unit, the Management and EDP support value will change by 0.66. The positive sign of the beta suggests that there is a positive linear relationship between the Management and EDP support and the number of subordinates. This means that the higher the number of subordinates reporting to a manager, the more should be the support of management and EDP staff provided to them. This contradicts the traditional view that the higher the span of control, the higher would be the number of relationships and, thus the less would be the level of control exercised upon and the degree of support provided to subordinates[36]. However, nowadays, defining an optimal role for MIS departments in this new computerized environment has been a difficult task for most companies,

---

36 George R. Terry, Principles of Management, London: IRWI- DORSEY INTERNATIONAL, 1972, P.P.388.

and thus MIS managers and users are being forced to reassess their traditional roles and relationships. This supports the findings reached by Kwan and Curley that showed the emergence of a "new partnership" in the corporate processing environment based on a set of clear roles, responsibilities and relationships between the MIS department and users[37]. MIS managers should provide necessary support to their subordinates to mantain data integrity and to avoide threats to IS that might be the result of intentional or accidental actions by a subordinate that did not receive support or is not under the MIS manger control and direction. Therefore, as the number of subordinates increase, it is very important for MIS managers to exert more effort to assist them.

### 4.11.3 Building a Regression Equation with Preventive Procedures Followed Being the Dependent Variable:

For this analysis, the same procedure was also followed with the same previously mentioned independent variables and with preventive procedures followed being the dependent variable. The correlation matrix is shown in Table XXXIII. As could be interestingly noticed, there is no significant correlation between any of the independent variables and the dependent variable. As a result, no regression equation could have been built here to determine the factors that are most likely to be associated with explaining the variation in the preventive procedures applied. This could be attributed to the fact that in our Lebanese organizations,

---

[37] Stephen K. Kwan and Kathleen Curley, "corporate MIS/DP and End User Computing: The Emergence of a New Partneship", Database, Summer 1989, p.p. 31-37

employees lack proper and complete understanding of such preventive methods, and are not really aware of their importance.

**Table XXXIII**
**Correlation Matrix between Preventive Procedures Followed and Independent Variables**

| □ | ZA | Z2 | X4 | X5 | X6 | X7 | X8 | X9 | X10 | X11 |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | | | □ |
| ZA | 1.000 | -.060 | .342 | .118 | .543 | .299 | .126 | -.165 | .340 | .340 |
| | | .435 | .166 | .373 | .052 | .201 | .364 | .324 | .169 | .169 |
| Z2 | -.060 | 1.000 | .478 | -.085 | .293 | .594 | .333 | .749 | -.098 | -.098 |
| | .435 | | .081 | .408 | .206 | .035 | .173 | .006 | .394 | .394 |
| X4 | .342 | .478 | 1.00 | .625 | .318 | .961 | .232 | .433 | .488 | .488 |
| | .166 | .081 | 0 | .027 | .185 | .000 | .260 | .106 | .076 | .076 |
| X5 | .118 | -.085 | .625 | 1.00 | -.165 | .502 | .282 | -.059 | .742 | .742 |
| | .373 | .408 | .027 | 0 | .324 | .069 | .215 | .435 | .007 | .007 |
| X6 | .543 | .293 | .318 | -.165 | 1.000 | .357 | .000 | .181 | .048 | .048 |
| | .052 | .206 | .185 | .324 | | .156 | .500 | .308 | .448 | .448 |
| X7 | .299 | .594 | .961 | .502 | .357 | 1.00 | .279 | .619 | .409 | .409 |
| | .201 | .035 | .000 | .069 | .156 | 0 | .217 | .028 | .120 | .120 |
| X8 | .126 | .333 | .232 | .282 | .000 | .279 | 1.000 | .134 | .163 | .163 |
| | .364 | .173 | .260 | .215 | .500 | .217 | | .356 | .327 | .327 |
| X9 | -.165 | .749 | .433 | -.059 | .181 | .619 | .134 | 1.00 | -.026 | -.026 |
| | .324 | .006 | .106 | .435 | .308 | .028 | .356 | 0 | .471 | .471 |
| X10 | .340 | -.098 | .488 | .742 | .048 | .409 | .163 | -.026 | 1.00 | 1.000 |
| | .169 | .394 | .076 | .007 | .448 | .120 | .327 | .471 | 0 | .000 |
| X11 | .340 | -.098 | .488 | .742 | .048 | .409 | .163 | -.026 | 1.00 | 1.000 |
| | .169 | .394 | .076 | .007 | .448 | .120 | .327 | .471 | 0 | |
| | | | | | | | | | .000 | |

### 4.11.4 Building a Regression Equation with Beliefs about Computer Threats and Crimes being the Dependent Variable:

To determine and analyze the factors that affect the beliefs of managers and users about computer crimes and threats, a regression model was built taking ZVI (Beliefs about Computer Threats and Crimes) as the dependent variable and the other variables as independent variables.

**Table XXXIV**
**Correlation Matrix between beliefs about Computer Threats and Crimes and Independent Variables**

| □ | ZVI | Z2 | X4 | X5 | X6 | X7 | X8 | X9 | X10 | X11 □ |
|---|---|---|---|---|---|---|---|---|---|---|
| ZVI | 1.000 | -.784 | -.667 | -.373 | .024 | -.740 | -.523 | -.706 | -.096 | -.096 |
| | | .004 | .018 | .144 | .474 | .007 | .060 | .011 | .396 | .396 |
| Z2 | -.784 | 1.000 | .478 | -.085 | .293 | .594 | .333 | .749 | -.098 | -.098 |
| | .004 | | .081 | .408 | .206 | .035 | .173 | .006 | .394 | .394 |
| X4 | -.667 | .478 | 1.00 | .625 | .318 | .961 | .232 | .433 | .488 | .488 |
| | .018 | .081 | 0 | .027 | .185 | .000 | .260 | .106 | .076 | .076 |
| X5 | -.373 | -.085 | .625 | 1.00 | -.165 | .502 | .282 | -.059 | .742 | .742 |
| | .144 | .408 | .027 | 0 | .324 | .069 | .215 | .435 | .007 | .007 |
| X6 | .024 | .293 | .318 | -.165 | 1.000 | .357 | .000 | .181 | .048 | .048 |
| | .474 | .206 | .185 | .324 | | .156 | .500 | .308 | .448 | .448 |
| X7 | -.740 | .594 | .961 | .502 | .357 | 1.00 | .279 | .619 | .409 | .409 |
| | .007 | .035 | .000 | .069 | .156 | 0 | .217 | .028 | .120 | .120 |
| X8 | -.523 | .333 | .232 | .282 | .000 | .279 | 1.000 | .134 | .163 | .163 |
| | .060 | .173 | .260 | .215 | .500 | .217 | | .356 | .327 | .327 |
| X9 | -.706 | .749 | .433 | -.059 | .181 | .619 | .134 | 1.00 | -.026 | -.026 |
| | .011 | .006 | .106 | .435 | .308 | .028 | .356 | 0 | .471 | .471 |
| X10 | -.096 | -.098 | .488 | .742 | .048 | .409 | .163 | -.026 | 1.00 | 1.000 |
| | .396 | .394 | .076 | .007 | .448 | .120 | .327 | .471 | 0 | .000 |
| X11 | -.096 | -.098 | .488 | .742 | .048 | .409 | .163 | -.026 | 1.00 | 1.000 |
| | .396 | .394 | .076 | .007 | .448 | .120 | .327 | .471 | 0 | |
| | | | | | | | | | .000 | |

The correlation matrix shown in table XXXIV reveals that there is a strong correlation between the dependent variable ZVI and the independent variables: organizational level (-0.784), years in organization (-0.667), number of subordinates (-0.373), age (-0.740), and the total number of employees (-0.706). The resulting regression model included two variables, the organizational level (Z2) and the number of subordinates (X5). The final regression output was as follows.

**Table XXXV**
**Regression Output-Dependent Variable=ZVI**

Variable (s) Entered on Step Number
1.. X5

| | |
|---|---|
| Multiple R | .89983 |
| R Square | .80970 |
| Adjusted R Square | .75533 |
| Standard Error | 1.06345 |

Analysis of Variance

| | DF | Sum of Squares | Mean Square |
|---|---|---|---|
| Regression | 2 | 33.68345 | 16.84173 |
| Residual | 7 | 7.91655 | 1.13094 |

F= 14.89186 Signif F= .0030

The coefficient of the independent variables are the beta values listed in table XXXVI. As a result, the regression equation that could be built for predicting beliefs about computer threats and crimes is:

$$ZVI=18.24 - 0.8218Z2 - 0.4424X5$$

$$(0.0000)\ (0.0016)\ \ (0.0318)$$

$$R^2= 0.80970= 80.97\%= 81\%$$

**Table XXXVI**
**Beta Coefficients and the Test for**
**Significance of the Independent Variable**

| Variable | Beta | T | Sig. T |
|---|---|---|---|
| Z2 | -0.821854 | -4967 | 0.0016 |
| X5 | -0.442393 | -2.673 | 0.0318 |
| (constant) | 18.238849 | 32.011 | 0.0000 |

A- The Significance of the Overall Regression Model.

The R square is given in the computer printout as 0.8097. This means that almost 81% of the variation in the beliefs about computer threats and crimes could be attributed to the two independent variables included in the model. Furthermore, to test the model significance, the critical F value < significance level, then the regression model could be considered significant.

B- The Significance of the Individual variables.

The significance of each independent variable will be again tested using the t- test. The t- values which are shown in table XXXVI, and put in parentheses under each independent variable are all less than the value of the level of significance, which is 0.05.

C- Interpretation of the Equation.

The analysis of the regression equation and the variables included in it could be done as follows. As for organizational level, the beta coefficient is 0.8218, indicating that, holding other variables constant, if

organizational level changes by one unit, then beliefs about computer threats and crimes will change by the value of 0.8218. This means that the level in the organizational hierarchy has a high influence on the beliefs and attitudes of employees towards computer crimes and threats. The negative sign of the beta suggests that there is a negative linear relationship between beliefs about computer threats and crimes and the organizational level. Such a negative relationship could be attributed to the fact that as the organizational level becomes higher, the concern of manager would be more directed towards global corporate issues in the organization like planning, budgeting, seeking new market segments and targets, tracing new opportunities in the market, and so on. Such involvement that requires a lot of time and attention would make managers at higher levels be less aware of possible threats that the organization might face in the computer and information system fields. Usually, people who directly interact with computers and information systems are expected to have more knowledge about computer threats, the level of security available, and the one they should have. Even such issues are communicated to the top management people, they might not be given the proper concern since they might be underestimated and looked at as real problems. Such a thing, among other things, might lead certain organizations at the end to consider technology as a cost rather than an asset.

The other factor that is included in the equation is the number of subordinates. Again here, the negative beta coefficient indicates that as the number of subordinates increases, the greater would be the number of

relationships and problems the supervisor should control and handle. This might lead the supervisor to be more busy with these issues than with handling problems such as computer crimes and threats, especially if the belief at the first place was against installing and using a computer system. Thus, as the span of control increases, the importance given to such issues would be less.

### 4.11.5 Building a Regression Equation with Suggested Viruses Intrusion Prevention Methods and Applied Prevention Methods Being the Dependent Variable:

Computer viruses are a major threat to computer operation and performance and have of course big influence on the successful implementation of computerized information systems, thus methods suggested and used to prevent intrusion of computer viruses are highly relevant in this study . The intention, here, was to develop regression models to investigate the factors that are most likely to be associated with the selection of prevention methods both suggested and applied.

To start with the suggested prevention methods (Z5A), of all the independent variables, the total number of employees (X9) was the only independent variable that was included in the regression model here. The regression output was as follows :

**Table XXXVII**
**Regression Output-Dependent Variable=Z5A**

Variable (s) Entered on Step Number
1.. X9

| | |
|---|---|
| Multiple R | .72203 |
| R Square | .52133 |
| Adjusted R Square | .46149 |
| Standard Error | 3.84601 |

Analysis of Variance

| | DF | Sum of Squares | Mean Square |
|---|---|---|---|
| Regression | 1 | 129.08079 | 129.08079 |
| Residual | 8 | 118.51921 | 14.81490 |

F= 8.71290 Signif F= .0184

The coefficient of the variable is shown in table XXXVIII. Based on this, the equation would be like this:

$$Z5A=35.4187 + 0.72203X9$$

$$(0.0000) \quad (0.0184)$$

$$R^2= 0.52133= 52.1\%$$

**Table XXXVIII**
**Beta Coefficients and the Test for**
**Significance of the Independent Variable**

| Variable | Beta | T | Sig. T |
|---|---|---|---|
| X9 | 0.722030 | 2.952 | .0184 |
| (constant) | 35.4187 | 21.191 | 0.0000 |

As for the applied prevention methods (Z5B), it is interesting to find that the total number of employees (X9) also was the only independent variable to be included in the model. The regression output was as follows

**Table XXXIX**
**Regression Output-Dependent Variable=Z5B**

Variable (s) Entered on Step Number
1.. X9

| | |
|---|---|
| Multiple R | .68157 |
| R Square | .46453 |
| Adjusted R Square | .39760 |
| Standard Error | 6.91305 |

Analysis of Variance

| | DF | Sum of Squares | Mean Square |
|---|---|---|---|
| Regression | 1 | 331.67745 | 331.67745 |
| Residual | 8 | 382.32255 | 47.79032 |

F= 6.94026 Signif F= .0300

The coefficient of the variable X9 in this case is shown in table XXXX, the regression equation would thus be:

$$Z5B=37.42 - 0.6815X9$$

$$(0.0000)\ (0.0300)$$

$$R^2= 0.46.453= 46.4\%$$

**Table XXXX**
**Beta Coefficients and the Test for Significance of the Independent Variable**

| Variable | Beta | T | Sig. T |
|---|---|---|---|
| X9 | -0.681567 | -2.634 | 0.0300 |
| (constant) | 37.420125 | 12.465 | 0.0000 |

A- The Significance of the Overall Regression Model.

The coefficient of determination, $R^2$, for Z5A was 0.52133, i.e., 52.13% of the variations in suggestions for virus prevention method could be explained by the total number of employees. On the other hand, 0.4645, i.e., 46.45% of the variations in methods of prevention applied could be attributed to total number of employees. In both equations, the model proved to be significant, since critical F < significant level.

For Z5A: F critical= 0.0184 < Sig. level= 0.05

For Z5B: F critical= 0.0300 < Sig. level= 0.05

B- The Significance of the Independent Variable.

The same procedure applied before will be used here to test the significance of independent variable. In both equations, where X9, the total number of employees, was the only respondent variable, the value of

the sig. t was less than the significance level, which means that X9 is a significant variable influencing Z5A and Z5B.

For Z5A: Sig. t= 0.0184 < Sig. level= 0.05

For Z5B: Sig. t= 0.0300 < Sig. level= 0.05

C- Interpretation of the Equations.

In the first equation, concerning Z5A, the beta coefficient has a value of 0.72030 indicating that if the total number of employees in the organization changes by one unit, the suggested methods of prevention variable would change by 0.72030. The positive sign indicates the positive linear relationship between the two variables. As for the second equation concerning Z5B, the applied methods against infection by computer viruses, the negative sign of the coefficient of the independent variable X9 indicates the negative linear relationship between the two variables. To begin with, a large number of employees would indicate a big organization. Regarding suggestions concerning the preventive methods that should be adopted, the bigger the size of the organization, the wider would be the scope of suggestions received by the various employees. This is logical since bigger organizations have high capital, sales, profits, ..., and of course an IS. Respondents in large organizations are more aware of the increasing risk of their information system. Take an example here a very large organization like MEA. If any disturbance takes place in the IS or computer database, the whole organization will be adversely affected.

The second equation concerning applied method support the hypothesis that the majority of big organizations in Lebanon are aware of the threats that might endanger their IS, but do not apply them in their organization. This could be attributed to the situation both economic and political, that has been prevailing in Lebanon for certain previous years. This led organizations, especially big ones, to concentrate on survival and re-establishment issues more than on computer security issues. The objective of increasing profit was found to be the most important, and sometimes the only objective of the organization. Only recently, after a period of peace and economic stability, organizations started to focus on other issues like computerization. This fact is recognized by people involved in marketing and business in general. A boom in computer sales and installation has been witnessed in Lebanon the last three years. This process is easily adopted by small companies. Thus, these companies had more time to test, evaluate, conclude, and adopt some preventive methods which usualy require lowest budget and a shortest period of time to implement than big organizations need. Moreover, big organizations are still witnessing the final stages of their computer installation.

With such a trend of computerization getting increased, and with the level of awareness that is supposed to accompany this trend becoming higher, dealing with issues of security, computer crimes, threats and pitfalls will be expected to come to the picture and be more and more considered.

This chapter provided a detailed analysis of all the findings of this study. A part of the findings conform with the literature reviewed, while the other part showed some inconsistencies with the findings provided by previous researches.

# CHAPTER V

## CONCLUSION AND RECOMMENDATION

### 5.1 Conclusion.

Eventhough it is a relatively new phenomenon, computer crimes and security measures for preventing these crimes have been the subject of many works of research. The risk and concern about computer crimes have been increasing in the last decade and leading to numerous inquisitions about the situation of computer security in the world and within organizations.

For the past three or four years, Lebanon has been witnessing a real boom towards computerization, and this fact is spread through various organizations belonging to different economic sectors. The majority of Lebanese organizations, small and big, have now their own IS, however, they are still unaware of how to give the proper attention towards computer security issues.

In this research, computer crimes and security measures were investigated. The outcome of this investigation supplied the researcher with a perception about the various aspects related to computer crimes and security. First, a major finding is that data processing budget, and especially data processing security budget were almost skipped in the annual budget of the organization, and in case they were included, they were given a very low percentage.

Another important finding is that approximately all respondents had free access to the system and had acquired their training and skills through self study, i.e., there was an absence of in house and outside or vender training.

The issue of "Improving security measures for IS" was ranked third among a list of ten issues, which means that respondents are becoming more aware about the importance of this issue. Furthermore, they have indicated that employee's behavior and performance are the main threat to computer security. Moreover, a high percentage of respondents indicated the superior risk that networks are exposed to in comparison with other environment.

Another finding reveals that big portion of Lebanese organization had witnessed virus disruption of their IS with a considerable percentage rejecting the fact that the issue of viruses was a concern in their organization. Nevertheless, if the organization was concerned and had applied some preventive measures, it was found that backup, passwords, and viruses scanning software, with the absence of new methods, applied outside Lebanon like auto terminal/account logoff, and control of workstations, were the most commonly used.

The regression analysis was performed to identify the factors that are most likely to be associated with the attainment of better security levels and with the avoidance of computer threats and pitfalls. The underlying approach here was to reach this objective indirectly through

studying factors such as job and career attitudes, management and EDP support, beliefs about computer threats and crimes, suggested prevention methods, and applied prevention methods. The assumption was that if employees have good career attitudes and are satisfied with their jobs, if management and the IS department are providing employees with the adequate and efficient support, if the organization people are well aware of the threats that the computer environment might be subject to, and if sufficient and effective prevention methods are applied and followed, then an efficient information system with reliable security measures can be provided to the organization. That's why the approach was to study these factors, consider each one as a dependent variable, and determine the factors that affect them. As a result, five regression equations were built. The first related age to career and job attitudes. The coefficient of determination, $R^2$ was 53.13% indicating that 53.13% of the variation in career and job attitudes could be explained by age. The second regression equation related Management and EDP support to number of subordinates. $R^2$ here was 43.6%, pointing that 43.6% of the variation in Management and EDP support could be attributed to number of subordinates. Concerning beliefs about computer threats and crime, it was found that this variable is affected by organizational level and number of subordinates with an $R^2$ of 81%. Finally, 2 regression equation were built concerning suggested and applied viruses prevention methods. In both equations, the total number of employees was the only determining variable that was included in the model. For the suggested prevention methods, $R^2$ was 52.1%, and for the applied ones, $R^2$ was 46.4%.

## 5.2 Limitations of the Study.

Two basic limitations were identified. First, the concept of computer security was viewed as a difficult technical concept by most Lebanese organizations. The level of understanding and acquaintance with this concept was very low. Second, information managers restrained from giving data concerning security problems and preventive methods applied in their departments either because of the privacy of the data and security system or because they want to conceal the existing pitfalls for which they are responsible.

## 5.3 Recommendations.

. An important recommendation is for managers to become more aware of security related issues. Training and seminars should be provided to increase this awareness and to introduce new preventive techniques that are used outside Lebanon in countries that have long experience in this field. Also training should be emphasized in the form of in-house and vendor training rather than self study.

Another recommendation is to prohibit free access and physical connection between mainframe and PC. Passwords IDs, and transaction logs should be used to limit free access, and to record any attempts of illegitimate access. More emphasis should be given to network security since it is the most vulnerable to threats.

IS managers should provide more support to their subordinates and end users. Moreover, orientation plans that provides information

IS managers should provide more support to their subordinates and end users. Moreover, orientation plans that provides information about the IS and the security system applied to protect this IS, should be implemented to direct new employees and prevent misapplication and corruption of the IS due to ignorance and unfamiliarity with the system. IS managers should set up disaster recovery policies and appoints a computer security officer to check integrity of the data, possible attempts to manipulate or misuse data, and so on.

Further research, that would take the above mentioned limitations into consideration, is needed, and thus it would expand the area of data gathering to have access to more information concerning the issue of computer security. Moreover, it is recommended for further research that researchers use a random sample selected from population (representative sample), and it is imperative to establish the construct validity of the instruments.

# APPENDIX A

# A SAMPLE QUESTIONNAIRE

# QUESTIONNAIRE.

My name is Houssam Tabbara. I am a graduate student at Beirut University College (BUC). I am conducting a study about computer crimes and the security measures related to this issue in Lebanon.

Your answers will be completely confidential, and the responses will be used purely for academic purposes.

Thank you.

# QUESTIONNAIRE

## PART I. General Information.

### A- Demographic Characteristics.

These questions are about your background and work experience.

1. What is your functional area?

| | | | |
|---|---|---|---|
| -----1. Acctg. | -----4. Gen. Mgmt | -----7. Sales | -----10. R&D |
| -----2. Finance | -----5. Personnel | -----8. Mfg./prod. | -----11. Other---------- |
| -----3. Eng'g. | -----6. Inf. System | -----9. Marketing | |

2. What is your level in the organization's hierarchy ?

| | |
|---|---|
| -----1. Prof. staff | -----4. St. Management |
| -----2. First level supervisor | -----5. Other---------- |
| -----3. Middle management | |

3. What is your primary organization's business ?

| | | |
|---|---|---|
| -----1. Mfg. | -----4. Public sector | -----7. Educational |
| -----2. Utility (Electronic, Gas) | -----5. Health care | -----8. Fin. services |
| -----3. Merchandising | -----6. Insurance | -----9. Other---------- |

4. Years in organization:---------- 5. Number of subordinates reporting to you:----------

6. Years of education:---------- 7. Age:---------- 8. Gender:----------

9. Total number of employees in the organization:----------

10. Data processing budget as an average percentage of the total annual budget:--------%

11. Size of the IS security budget as an average percent of the DP budget:--------%

### B- Computer Use.

**If you are not using a PC, please go to part B.**

**Part A.**

1. Personal Computer: Type

----- 1. Stand alone ----- 2. Connected to other computer or networks

2. Is it your own computer? -----1. Yes -----2. No

3. Do you have free access? -----1. Yes -----2. No

**Part B.**

1. Are you using non-PC (Mainframe or minicomputer)? -----1. Yes -----2. No

**Part C.**

1. On an average weekly day that you use a computer, how much time do you spend on the system?

-----1. 0 under 2 hours -----2. 2 under 4 hours
-----3. 4 under 6 hours -----4. 6 under 8 hours

2. On the average how frequently do you use a computer per month?

-----1. 0 under 5 days -----2. 5 under 10 days -----3. 10 under 15 days
-----4. 15 under 20 days -----5. 20 under 25 days -----6. 25 under 30 days

3. For how long have you been using the system?

-----Years

## C-.Computer Training.

Which of the following categories best describe the level of training you have had in the use of computers, both mainframe and/or microcomputers.

| | none | | | | Extensive |
|---|---|---|---|---|---|
| 1. General courses at college or university. | 1 | 2 | 3 | 4 | 5 |
| 2. Training provided by vendors or outside consultants. | 1 | 2 | 3 | 4 | 5 |
| 3. In house company courses. | 1 | 2 | 3 | 4 | 5 |
| 4. Through self study. | 1 | 2 | 3 | 4 | 5 |

## D- Computer knowledge and Experience.

The next set of questions assesses the actual experience you have been working with computers and your knowledge about computers in general.

1. How many courses have you taken in computers?----------
2. For how long have you used PCs?----------years.
3. For how long have you used computers in general?----------years.
4. For how long have you written programs in computer language?----------years.

## PART II. Information System Management.

Please rank the **top 3** of the following **10** issues for Information System Management, according to their importance.

----- 1. Improved information system planning.
----- 2. Management and facilitation of end user computing.
----- 3. Integration of data processing, office automation, and telecommunications.
----- 4. Improved software development and quality.
----- 5. Improving security measures for information systems.
----- 6. Facilitation of organizational learning and use of information system technologies.
----- 7. Alignment of the IS organization with that of the enterprise.
----- 8. Specification, recruitment, and development of IS human resources.
----- 9. Effective use of the organization's data resources.
-----10. Development and implementation of decision support systems.

## PART III. Threats to Information Systems Security.

Please rank the **top 3** of the following **12** threats to the security of your organization's Information System(s).

----- 1. Accidental entry of 'bad' data by employees.
----- 2. Intentional entry of 'bad' data by employees.
----- 3. Accidental destruction of data by employees.
----- 4. Intentional destruction of data by employees.
----- 5. Unauthorized access to data/system by employees.
----- 6. Inadequate control over media (disks, tapes).
----- 7. Poor control over manual handling of I/O.
----- 8. Access to data/system by outsiders(hackers).
----- 9. Access to data/system by outsiders(competitors).
-----10. Entry into system of computer viruses.
-----11. Weak, ineffective, inadequate physical control.
-----12. Natural disaster, loss of power, communications.
-----13. Other:----------

Please evaluate your organization's risk of computer disruption in each of the following environments.

1= V. low risk 2= low risk 3= Moderate risk 4= High risk 5= V. high risk

-----Microcomputer
-----Network
-----Mainframe (or minicomputer)
-----The overall risk of computer disruption

## PART IV. Computer viruses relative to other threats

1. Has your organization had any verified incidents of computer disruption due to the intrusion of computer viruses? -----Yes -----No

2. Please evaluate your organization's risk of computer disruption on your information system due to the intrusion of computer viruses?

-----1. V. high -----3. Moderate -----5. V. low
-----2. High -----4. Low

3. The issue of computer viruses is not a major concern in my organization.

-----1. Strongly disagree -----3. Neutral -----5. Strongly agree
-----2. Disagree -----4. Agree

## PART V. Computer Viruses Prevention.

**A-** The following statements are suggestions for certain aspects that could be followed to prevent infection by computer viruses. Please circle the choice that best fits your opinion about whether each aspect is efficient to achieve this purpose:

1= Strongly Agree
2= Agree
3= Undecided
4= Disagree
5= Strongly disagree

| | | | | | |
|---|---|---|---|---|---|
| 1- The use of passwords | 1 | 2 | 3 | 4 | 5 |
| 2- Backup procedures schedules | 1 | 2 | 3 | 4 | 5 |
| 3- Employee education | 1 | 2 | 3 | 4 | 5 |
| 4- Consistent security policies | 1 | 2 | 3 | 4 | 5 |
| 5- company-provided software only | 1 | 2 | 3 | 4 | 5 |
| 6- Use of virus scanning software | 1 | 2 | 3 | 4 | 5 |
| 7- Audit procedures strengthened | 1 | 2 | 3 | 4 | 5 |
| 8- Monitor computer user usage | 1 | 2 | 3 | 4 | 5 |
| 9- Auto terminal/account logoff | 1 | 2 | 3 | 4 | 5 |
| 10- No outside connections | 1 | 2 | 3 | 4 | 5 |
| 11- Publish formal standards | 1 | 2 | 3 | 4 | 5 |
| 12- Reporting violations encouraged | 1 | 2 | 3 | 4 | 5 |
| 13- Control of workstations | 1 | 2 | 3 | 4 | 5 |
| 14- Ethics training | 1 | 2 | 3 | 4 | 5 |

15- Other, specify----------

**B-**In this section, for each of the following actions designed to prevent infection by computer viruses, please indicate the extent to which each action is applied in your orgnization.

| | Not at all | | | | To a great extent |
|---|---|---|---|---|---|
| 1- The use of passwords | 1 | 2 | 3 | 4 | 5 |
| 2- Backup procedures schedules | 1 | 2 | 3 | 4 | 5 |
| 3- Employee education | 1 | 2 | 3 | 4 | 5 |
| 4- Consistent security policies | 1 | 2 | 3 | 4 | 5 |
| 5- company-provided software only | 1 | 2 | 3 | 4 | 5 |
| 6- Use of virus scanning software | 1 | 2 | 3 | 4 | 5 |
| 7- Audit procedures strengthened | 1 | 2 | 3 | 4 | 5 |
| 8- Monitor computer user usage | 1 | 2 | 3 | 4 | 5 |
| 9- Auto terminal/account logoff | 1 | 2 | 3 | 4 | 5 |
| 10- No outside connections | 1 | 2 | 3 | 4 | 5 |
| 11- Publish formal standards | 1 | 2 | 3 | 4 | 5 |
| 12- Reporting violations encouraged | 1 | 2 | 3 | 4 | 5 |
| 13- Control of workstations | 1 | 2 | 3 | 4 | 5 |
| 14- Ethics training | 1 | 2 | 3 | 4 | 5 |
| 15- Other, specify---------- | | | | | |

## PART VI. Beliefs about Computer Threats & Crimes.

In this section, we would like to find out what you believe is the state of computer crimes at present. Please circle one number of each statement which corresponds mostly to your desired response.

1= Strongly Disagree
2= Disagree
3= Undecided
4= Agree
5= Strongly Agree

| | | | | | |
|---|---|---|---|---|---|
| 1. Using a computer allows me to access information from any place without difficulties. | 1 | 2 | 3 | 4 | 5 |
| 2. Using a computer exposes me to vulnerability of computer breakdown and loss of data. | 1 | 2 | 3 | 4 | 5 |
| 3. In my opinion, 10 years ago, it was hard for the user to manipulate things on the computer. Today, it's very easy for a novice to break security. | 1 | 2 | 3 | 4 | 5 |

| | | | | | |
|---|---|---|---|---|---|
| 4. Distributed systems exposes data and program files to threats more than the centralized systems do. | 1 | 2 | 3 | 4 | 5 |
| 5. The use of stand alone processors can greatly aid in the theft procedures, especially copying programs and data etc. | 1 | 2 | 3 | 4 | 5 |

# PART VII. Organizations' Policies and Measures.

## A- Preventive procedures followed

This section is used to evaluate the various procedures applied in your organization to prevent or reduce computer crimes. Please circle one number of each statement which corresponds mostly to your desired response.

1= Strongly Disagree
2= Disagree
3= Undecided
4= Agree
5= Strongly Agree

| | | | | | |
|---|---|---|---|---|---|
| 1. Important job functions are well separated. | 1 | 2 | 3 | 4 | 5 |
| 2. Users don't have free access to information from any place in the organization through the computer system they are using. | 1 | 2 | 3 | 4 | 5 |
| 3. Each job function is handled by one person only, or by a well defined group of employees. | 1 | 2 | 3 | 4 | 5 |
| 4. In case of errors in performance and job handling, accountability and responsibility can be well determined. | 1 | 2 | 3 | 4 | 5 |
| 5. Physical access to computer systems is well controlled. | 1 | 2 | 3 | 4 | 5 |
| 6. Time restrictions and workstation restrictions are used to enhance the control of physical access to computer systems. | 1 | 2 | 3 | 4 | 5 |
| 7. Auditors of information systems are available to control the use of computer systems by various users. | 1 | 2 | 3 | 4 | 5 |

| | | | | | |
|---|---|---|---|---|---|
| 8. At the end of each day, information auditors check and control all transactions done by various users during the day. | 1 | 2 | 3 | 4 | 5 |
| 9. A transaction log equipped in the system keeps records of all users accessing the system, the time of access, and the type of transaction done by the user. | 1 | 2 | 3 | 4 | 5 |
| 10. Overall, adequate procedures are adopted to prevent computer crimes in our organization. | 1 | 2 | 3 | 4 | 5 |

## B- Management & Electronic Data Processing (EDP) Support.

The next section is used to assess management and EDP support to Information Systems Security. Please circle one number of each statement which corresponds mostly to your desired response.

1= Strongly Disagree
2= Disagree
3= Undecided
4= Agree
5= Strongly Agree

| | | | | | |
|---|---|---|---|---|---|
| 1. A central support (e.g. information center) is available to help with problems. | 1 | 2 | 3 | 4 | 5 |
| 2. I am convinced that management is sure as to what risks can threaten the computer system. | 1 | 2 | 3 | 4 | 5 |
| 3. There is always a person in the organization whom we can turn to for help in solving with the computer system. | 1 | 2 | 3 | 4 | 5 |
| 4. Training courses are readily available for us to improve our awareness of computer threats. | 1 | 2 | 3 | 4 | 5 |
| 5. Management has provided most of the necessary help and resources to protect both the computer hardware and software against various threats | 1 | 2 | 3 | 4 | 5 |

| | | | | | |
|---|---|---|---|---|---|
| 6. We are constantly updated on new methods that can help in enhancing the computer security. | 1 | 2 | 3 | 4 | 5 |
| 7. Management is really keen to see that good security measures are always applied in the organization | 1 | 2 | 3 | 4 | 5 |

## C- Career & Job Attitudes

Please circle one number of each statement which corresponds mostly to your desired response.

1= Strongly Disagree
2= Disagree
3= Undecided
4= Agree
5= Strongly Agree

| | | | | | |
|---|---|---|---|---|---|
| 1. I am satisfied with the success I have achieved in my career. | 1 | 2 | 3 | 4 | 5 |
| 2. I am satisfied with the progress I have made toward achieving my overall career goals. | 1 | 2 | 3 | 4 | 5 |
| 3. If I had to do it all over again, I would have made the same career choices I have made. | 1 | 2 | 3 | 4 | 5 |
| 4. Overall, I would say that my personal needs have been met with my present career. | 1 | 2 | 3 | 4 | 5 |
| 5. I am satisfied with the promotion rate in my career. | 1 | 2 | 3 | 4 | 5 |
| 6. I would advise many of my friends to apply to this organization. | 1 | 2 | 3 | 4 | 5 |
| 7. I never think of changing my job. | 1 | 2 | 3 | 4 | 5 |
| 8. I am usually satisfied with my job. | 1 | 2 | 3 | 4 | 5 |

I would like to thank you for your time , interest, and patience in answering this questionnaire. Your answers are central to the success of this research. When you are finished, please return the survey to the person who is conducting this effort.

# APPENDIX B

# LIST OF REGRESSION ANALYSIS OUTPUT

* * * * M U L T I P L E R E G R E S S I O N * * * *

Listwise Deletion of Missing Data

| | Mean | Std Devi | Label |
|---|---|---|---|
| ZCA | 3.050 | .430 | |
| ZZ1 | 1.000 | .000 | |
| Z1 | 1.000 | .000 | |
| Z2 | .500 | .527 | |
| Z3 | .000 | .000 | |
| X4 | 6.200 | 4.849 | |
| X5 | 2.000 | 2.494 | |
| X6 | 22.000 | 2.160 | |
| X7 | 30.500 | 6.916 | |
| X8 | .900 | .316 | |
| X9 | 1742.500 | 1951.642 | |
| X10 | .500 | 1.080 | |
| X11 | .500 | 1.080 | |

N of Cases = 10

* * * * M U L T I P L E R E G R E S S I O N * * * *

Correlation, 1-tailed Sig:

' . ' is printed if a correlation cannot be computed.

| | ZCA | ZZ1 | Z1 | Z2 | Z3 | X4 | X5 | X6 |
|---|---|---|---|---|---|---|---|---|
| ZCA | 1.000 | . | . | .245 | . | .726 | .168 | .419 |
| | . | .000 | .000 | .247 | .000 | .009 | .321 | .114 |
| ZZ1 | . | 1.000 | . | . | . | . | . | . |
| | .000 | . | .000 | .000 | .000 | .000 | .000 | .000 |
| Z1 | . | . | 1.000 | . | . | . | . | . |
| | .000 | .000 | . | .000 | .000 | .000 | .000 | .000 |
| Z2 | .245 | . | . | 1.000 | . | .478 | -.085 | .293 |
| | .247 | .000 | .000 | . | .000 | .081 | .408 | .206 |
| Z3 | . | . | . | . | 1.000 | . | . | . |
| | .000 | .000 | .000 | .000 | . | .000 | .000 | .000 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | .009 | .000 | .000 | .081 | .000 | . | .027 | .185 |
| X5 | .168 | . | . | -.085 | . | .625 | 1.000 | -.165 |
| | .321 | .000 | .000 | .408 | .000 | .027 | . | .324 |
| X6 | .419 | . | . | .293 | . | .318 | -.165 | 1.000 |
| | .114 | .000 | .000 | .206 | .000 | .185 | .324 | . |
| X7 | .729 | . | . | .594 | . | .961 | .502 | .357 |
| | .008 | .000 | .000 | .035 | .000 | .000 | .069 | .156 |
| X8 | .041 | . | . | .333 | . | .232 | .282 | .000 |
| | .455 | .000 | .000 | .173 | .000 | .260 | .215 | .500 |
| X9 | .464 | . | . | .749 | . | .433 | -.059 | .181 |
| | .089 | .000 | .000 | .006 | .000 | .106 | .435 | .308 |
| X10 | .120 | . | . | -.090 | . | .488 | .742 | .048 |
| | .371 | .000 | .000 | .394 | .000 | .076 | .007 | .448 |
| X11 | .120 | . | . | -.090 | . | .488 | .742 | .048 |
| | .371 | .000 | .000 | .394 | .000 | .076 | .007 | .448 |

* * * * M U L T I P L E R E G R E S S I O N * * * *

| | X7 | X8 | X9 | X10 | X11 |
|---|---|---|---|---|---|
| XCA | .729 | .041 | .464 | .120 | .120 |
| | .008 | .455 | .089 | .371 | .371 |
| XB1 | . | . | . | . | . |
| | .000 | .000 | .000 | .000 | .000 |
| B1 | . | . | . | . | . |
| | .000 | .000 | .000 | .000 | .000 |
| B2 | .594 | .333 | .749 | -.090 | -.090 |
| | .035 | .173 | .006 | .394 | .394 |
| B3 | . | . | . | . | . |
| | .000 | .000 | .000 | .000 | .000 |
| X4 | .961 | .232 | .433 | .488 | .488 |
| | .000 | .260 | .106 | .076 | .076 |
| X5 | .502 | .282 | -.059 | .742 | .742 |
| | .069 | .215 | .435 | .007 | .007 |
| X6 | .357 | .000 | .181 | .048 | .048 |
| | .156 | .500 | .308 | .448 | .448 |

| | | | | | |
|---|---|---|---|---|---|
| | . | .217 | .028 | .120 | .120 |
| X8 | .279 | 1.000 | .134 | .163 | .163 |
| | .217 | . | .356 | .327 | .327 |
| X9 | .619 | .134 | 1.000 | -.026 | -.026 |
| | .028 | .356 | . | .471 | .471 |
| X10 | .409 | .163 | -.026 | 1.000 | 1.000 |
| | .120 | .327 | .471 | . | .000 |
| X11 | .409 | .163 | -.026 | 1.000 | 1.000 |
| | .120 | .327 | .471 | .000 | |

* * * * M U L T I P L E R E G R E S S I O N * * * *

Equation Number 1 Dependent Variable. X28

Descriptive Statistics are printed on Page 2

The following variables are constants or have missing correlations:

ZZ1 Z1 Z3

They will be deleted from the analysis.

Block Number 1. Method: Stepwise Criteria PIN .0500 POUT .1000

Z21 Z1 Z2 Z3 Z4 Z5 Z6 X7
X8 X9 X10 X11

| Step | MultR | Rsq | F(Eqn) | SigF | | Variable | RsqIn |
|---|---|---|---|---|---|---|---|
| 1 | .7289 | .5313 | 9.068 | .017 | In | X7 | .7289 |

Variable(s) Entered on Step Number
1.. X7

| | |
|---|---|
| Multiple R | .72890 |
| R Square | .53129 |
| Adjusted R Square | .47271 |
| Standard Error | .31209 |

Analysis of Variance

| | DF | Sum of Squares | Mean Square |
|---|---|---|---|
| Regression | 1 | .88328 | .88328 |
| Residual | 8 | .77922 | .09740 |

F = 9.06825 Signif F = .0160

| Variable | B | SE B | Beta | T | Sig T |
|---|---|---|---|---|---|
| X7 | .045296 | .015042 | .728899 | 3.011 | .0168 |
| (Constant) | 1.668467 | .460270 | | 3.625 | .0074 |

* * * * M U L T I P L E R E G R E S S I O N * * * *

Equation Number 1 Dependent Variable.. SCA

---------- Variables not in the Equation ----------

| Variable | Beta In | Partial | Min Toler | T | Sig T |
|---|---|---|---|---|---|
| Z2 | -.230713 | -.341477 | .646690 | -.961 | .3684 |
| X4 | .357021 | .144496 | .076776 | .386 | .7107 |
| X5 | -.264507 | -.334065 | .747636 | -.938 | .3796 |
| X6 | .181830 | .248094 | .872573 | .678 | .5198 |
| X8 | -.176578 | -.217647 | .921925 | -.676 | .5206 |
| X9 | .020058 | .023003 | .616729 | .061 | .9531 |
| X10 | -.214323 | -.285668 | .832697 | -.789 | .4562 |
| X11 | -.214323 | -.285668 | .832697 | -.789 | .4562 |

End Block Number 1 PIN = .050 Limits reached.

* * * * M U L T I P L E R E G R E S S I O N * * * *

Listwise Deletion of Missing Data

| | Mean | Std Dev | Label |
|---|---|---|---|
| ZB | 17.600 | 3.777 | |
| Z1 | 1.000 | .000 | |
| Z2 | .500 | .527 | |
| Z3 | .000 | .000 | |
| ZZ1 | 1.000 | .000 | |
| X4 | 6.200 | 4.849 | |
| X5 | 2.000 | 2.494 | |
| X6 | 22.000 | 2.160 | |
| X7 | 30.500 | 6.916 | |
| X8 | .900 | .316 | |
| X9 | 1742.500 | 1951.642 | |
| X10 | .500 | 1.080 | |
| X11 | .500 | 1.080 | |

N of Cases = 10

Correlation, 1-tailed Sig:

' . ' is printed if a correlation cannot be computed.

| | ZB | Z1 | Z2 | Z3 | ZZ1 | X4 | X5 | X6 |
|---|---|---|---|---|---|---|---|---|
| ZB | 1.000 | . | -.391 | . | . | .430 | .660 | -.327 |
| | . | .000 | .132 | .000 | .000 | .100 | .019 | .178 |
| Z1 | . | 1.000 | . | . | . | . | . | . |
| | .000 | . | .000 | .000 | .000 | .000 | .000 | .000 |
| Z2 | -.391 | . | 1.000 | . | . | .478 | -.085 | .293 |
| | .132 | .000 | . | .000 | .000 | .081 | .408 | .206 |
| Z3 | . | . | | 1.000 | . | . | . | . |
| | .000 | .000 | .000 | . | .000 | .000 | .000 | .000 |
| ZZ1 | . | . | . | . | 1.000 | . | . | . |
| | .000 | .000 | .000 | .000 | . | .000 | .000 | .000 |
| X4 | .430 | . | .478 | . | . | 1.000 | .625 | .318 |
| | .100 | .000 | .081 | .000 | .000 | . | .027 | .185 |
| X5 | 660 | . | -.085 | | . | .625 | 1.000 | -.165 |
| | .019 | .000 | .409 | 000 | .000 | .027 | . | .324 |
| X6 | -.327 | . | .293 | . | . | .318 | -.165 | 1.000 |
| | .178 | .000 | .206 | .000 | 000 | .185 | .324 | . |
| X7 | .379 | . | .594 | . | . | .961 | .502 | .357 |
| | .140 | .000 | .035 | .000 | .000 | .000 | .069 | .156 |
| X8 | .056 | . | .333 | . | . | .232 | .282 | .000 |
| | .439 | .000 | 173 | .000 | 000 | .260 | .215 | .500 |
| X9 | .015 | . | .740 | . | | .433 | -.059 | .181 |
| | .484 | .000 | .006 | .000 | .000 | .106 | .435 | .308 |
| X10 | .626 | . | .098 | . | . | .488 | .742 | .048 |
| | .026 | .000 | .394 | 000 | .000 | .076 | .007 | .448 |
| X11 | .626 | . | -.098 | . | . | .488 | .742 | .048 |
| | .026 | .000 | .394 | .000 | .000 | .076 | .007 | .448 |

* * * * M U L T I P L E R E G R E S S I O N * * * *

| | X7 | X8 | X9 | X10 | X11 |
|---|---|---|---|---|---|
| ZB | .379 | .056 | .015 | .626 | .626 |

| | | | | | |
|---|---|---|---|---|---|
| Z1 | . | . | . | . | . |
| | .000 | .000 | .000 | .000 | .000 |
| Z2 | .594 | .333 | .749 | -.098 | -.098 |
| | .035 | .173 | .006 | .394 | .394 |
| Z3 | . | . | . | . | . |
| | .000 | .000 | .000 | .000 | .000 |
| ZZ1 | . | . | . | . | . |
| | .000 | .000 | .000 | .000 | .000 |
| X4 | .961 | .232 | .433 | .499 | .488 |
| | .000 | .260 | .106 | .076 | .076 |
| X5 | .502 | .282 | -.059 | .742 | .742 |
| | .069 | .215 | .435 | .007 | .007 |
| X6 | .357 | .000 | .101 | .040 | .048 |
| | .156 | .500 | .308 | .448 | .448 |
| X7 | 1.000 | .279 | .619 | .499 | .409 |
| | . | .217 | .028 | .120 | .120 |
| X8 | .279 | 1.000 | .134 | .163 | .163 |
| | .217 | . | .356 | .327 | .327 |
| X9 | .619 | .134 | 1.000 | -.026 | -.026 |
| | .028 | .356 | . | .471 | .471 |
| X10 | .409 | .163 | -.026 | 1.000 | 1.000 |
| | .120 | .327 | .471 | . | .000 |
| X11 | .409 | .163 | -.026 | 1.000 | 1.000 |
| | .120 | .327 | .471 | .000 | . |

* * * * M U L T I P L E R E G R E S S I O N * * * *

Equation Number 1 Dependent Variable.. SB

Descriptive Statistics are printed on Page 7

The following variables are constants or have missing correlations:

Z1 Z3 ZZ1

They will be deleted from the analysis.

Block Number 1. Method: Stepwise Criteria PIN .0500 POUT .1000

Z1 Z2 Z3 ZZ1 X4 X5 X6 X7

| Step | MultR | Req | F(Eqn) | SigF | | Variable | BetaIn |
|---|---|---|---|---|---|---|---|
| 1 | .6604 | .4361 | 6.188 | .038 | In: | X5 | .6604 |

Variable(s) Entered on Step Number
1.. X5

| | |
|---|---|
| Multiple R | .66041 |
| R Square | .43611 |
| Adjusted R Square | .36565 |
| Standard Error | 3.00832 |

Analysis of Variance

| | DF | Sum of Squares | Mean Square |
|---|---|---|---|
| Regression | 1 | 56.00000 | 56.00000 |
| Residual | 8 | 72.40000 | 9.05000 |

F = 6.18785 Signif F = .0377

---------- Variables in the Equation ----------

| Variable | B | SE B | Beta | T | Sig T |
|---|---|---|---|---|---|
| X5 | 1.000000 | .402004 | .660407 | 2.488 | .0377 |
| (Constant) | 15.600000 | 1.245564 | | 12.524 | .0000 |

* * * * MULTIPLE REGRESSION * * * *

Equation Number 1 Dependent Variable.. EB

---------- Variables not in the Equation ----------

| Variable | Beta In | Partial | Min Toler | T | Sig T |
|---|---|---|---|---|---|
| X2 | -.337297 | -.447578 | .992857 | -1.324 | .2270 |
| X4 | .027858 | .028970 | .609776 | .077 | .9410 |
| X6 | -.223972 | -.294192 | .972789 | -.814 | .4423 |
| X7 | .062580 | .072060 | .747636 | .191 | .8538 |
| X8 | -.141461 | -.180756 | .920635 | -.486 | .6416 |
| X9 | .054530 | .072491 | .996465 | .192 | .8530 |
| X10 | .303296 | .270660 | .448980 | .744 | .4812 |
| X11 | .303296 | .270660 | .448980 | .744 | .4812 |

End Block Number 1 PIN = .050 Limits reached.

* * * * MULTIPLE REGRESSION * * * *

Listwise Deletion of Missing Data

| | Mean | Std Devi | Label |
|---|---|---|---|
| ZA | 28.900 | 5.391 | |
| ZS1 | 1.000 | .000 | |
| Z1 | 1.000 | .000 | |
| Z2 | .500 | .527 | |
| Z3 | .000 | .000 | |
| X4 | 6.200 | 4.849 | |
| X5 | 2.000 | 2.494 | |
| X6 | 22.000 | 2.160 | |
| X7 | 30.500 | 6.916 | |
| X8 | .900 | .316 | |
| X9 | 1742.500 | 1951.642 | |
| X10 | .500 | 1.080 | |
| X11 | .500 | 1.080 | |

N of Cases = 10

* * * * M U L T I P L E R E G R E S S I O N * * * *

Correlation, 1-tailed Sig:

' . ' is printed if a correlation cannot be computed.

| | ZA | ZS1 | Z1 | Z2 | Z3 | X4 | X5 | X6 |
|---|---|---|---|---|---|---|---|---|
| ZA | 1.000 | . | . | -.060 | . | .342 | .118 | .543 |
| | . | .000 | .000 | .435 | .000 | .166 | .373 | .052 |
| ZS1 | . | 1.000 | . | . | . | . | . | . |
| | .000 | . | .000 | .000 | .000 | .000 | .000 | .000 |
| Z1 | . | . | 1.000 | . | . | . | . | . |
| | .000 | .000 | . | .000 | .000 | .000 | .000 | .000 |
| Z2 | -.060 | . | . | 1.000 | . | .478 | -.085 | .293 |
| | .435 | .000 | .000 | . | .000 | .081 | .408 | .206 |
| Z3 | . | . | . | . | 1.000 | . | . | . |
| | .000 | .000 | .000 | .000 | . | .000 | .000 | .000 |
| X4 | .342 | . | . | .478 | . | 1.000 | .625 | .318 |
| | .166 | .000 | .000 | .081 | .000 | . | .027 | .185 |
| X5 | .118 | . | . | -.085 | . | .625 | 1.000 | -.165 |
| | .373 | .000 | .000 | .408 | .000 | .027 | . | .324 |
| X6 | .543 | . | . | .293 | . | .318 | -.165 | 1.000 |
| | .052 | .000 | .000 | .206 | .000 | .185 | .324 | . |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | .201 | .000 | .000 | .035 | .000 | .000 | .069 | .156 |
| X8 | .126 | . | . | .333 | . | .232 | .282 | .000 |
| | .364 | .000 | .000 | .173 | .000 | .260 | .215 | .500 |
| X9 | -.165 | . | . | .749 | . | .433 | -.059 | .181 |
| | .324 | .000 | .000 | .006 | .000 | .106 | .435 | .308 |
| X10 | .340 | . | . | -.098 | . | .498 | .742 | .048 |
| | .169 | .000 | .000 | .394 | .000 | .076 | .007 | .448 |
| X11 | .340 | . | . | -.098 | . | .408 | .742 | .048 |
| | .169 | .000 | .000 | .394 | .000 | .076 | .007 | .448 |

* * * * M U L T I P L E R E G R E S S I O N * * * *

| | X7 | X8 | X9 | X10 | X11 |
|---|---|---|---|---|---|
| ZA | .299 | .126 | -.165 | .340 | .340 |
| | .201 | .364 | .324 | .169 | .169 |
| ZZ1 | . | . | . | . | . |
| | .000 | .000 | .000 | .000 | .000 |
| Z1 | . | . | . | . | . |
| | .000 | .000 | .000 | .000 | .000 |
| Z2 | .594 | .333 | .749 | -.098 | -.098 |
| | .035 | .173 | .006 | .394 | .394 |
| Z3 | . | . | . | . | . |
| | .000 | .000 | .000 | .000 | .000 |
| X4 | .961 | .232 | .433 | .498 | .408 |
| | .000 | .260 | .106 | .076 | .076 |
| X5 | .502 | .282 | -.059 | .742 | .742 |
| | .060 | .215 | .435 | .007 | .007 |
| X6 | .357 | .000 | .181 | .048 | .048 |
| | .156 | .500 | .309 | .448 | .448 |
| X7 | 1.000 | .279 | .619 | .409 | .409 |
| | . | .217 | .028 | .120 | .120 |
| X8 | .279 | 1.000 | .134 | .163 | .163 |
| | .217 | . | .356 | .327 | .327 |
| X9 | .619 | .134 | 1.000 | -.026 | -.026 |
| | .028 | .356 | . | .471 | .471 |

```
            .120      .327      .471       .          .000

X11          .409      .163     -.026     1.000      1.000
             .120      .327      .471      .000        .
```

* * * *  M U L T I P L E  R E G R E S S I O N  * * * *

Equation Number 1  Dependent Variable..  ZA

Descriptive Statistics are printed on Page  12

The following variables are constants or have missing correlations:

ZZ1  Z1  Z3

They will be deleted from the analysis.

Block Number 1. Method: Stepwise  Criteria  PIN .0500  POUT .1000

ZZ1  Z1  Z2  Z3  X4  X5  X6  X7
X8  X9  X10  X11

End Block Number 1  PIN = .050 Limits reached.
No variables entered/removed for this block.

* * * *  M U L T I P L E  R E G R E S S I O N  * * * *

Listwise Deletion of Missing Data

| | Mean | Std Devi | Label |
|---|---|---|---|
| ZV1 | 15.800 | 2.150 | |
| ZZ1 | 1.000 | .000 | |
| Z1 | 1.000 | .000 | |
| Z2 | .500 | .527 | |
| Z3 | .000 | .000 | |
| X4 | 6.200 | 4.849 | |
| X5 | 2.000 | 2.494 | |
| X6 | 22.000 | 2.160 | |
| X7 | 30.500 | 6.916 | |
| X8 | .900 | .316 | |
| X9 | 1742.500 | 1951.642 | |
| X10 | .500 | 1.080 | |
| X11 | .500 | 1.080 | |

N of Cases = 10

* * * * M U L T I P L E R E G R E S S I O N * * * *

Correlation, 1-tailed Sig:

' . ' is printed if a correlation cannot be computed.

| | ZV1 | ZZ1 | Z1 | Z2 | Z3 | X4 | X5 | X6 |
|---|---|---|---|---|---|---|---|---|
| ZV1 | 1.000 | . | . | -.784 | . | -.667 | -.373 | .024 |
| | . | .000 | .000 | .004 | .000 | .018 | .144 | .474 |
| ZZ1 | . | 1.000 | . | . | . | . | . | . |
| | .000 | . | .000 | .000 | .000 | .000 | .000 | .000 |
| Z1 | . | . | 1.000 | . | . | . | . | . |
| | .000 | .000 | . | .000 | .000 | .000 | .000 | .000 |
| Z2 | -.784 | . | . | 1.000 | . | .478 | -.085 | .293 |
| | .004 | .000 | .000 | . | .000 | .081 | .408 | .206 |
| Z3 | . | . | . | . | 1.000 | . | . | . |
| | .000 | .000 | .000 | .000 | . | .000 | .000 | .000 |
| X4 | -.667 | . | . | .478 | . | 1.000 | .625 | .318 |
| | .018 | .000 | .000 | .081 | .000 | . | .027 | .185 |
| X5 | -.373 | . | . | -.085 | . | .625 | 1.000 | -.165 |
| | .144 | .000 | .000 | .408 | .000 | .027 | . | .324 |
| X6 | .024 | . | . | .293 | . | .318 | -.165 | 1.000 |
| | .474 | .000 | .000 | .206 | .000 | .185 | .324 | . |
| X7 | -.740 | . | . | .594 | . | .961 | .502 | .357 |
| | .007 | .000 | .000 | .035 | .000 | .000 | .069 | .156 |
| X8 | -.523 | . | . | 333 | | .232 | .282 | .000 |
| | .060 | .000 | .000 | .173 | .000 | .260 | .215 | .500 |
| X9 | -.706 | . | . | .749 | . | .433 | -.059 | .181 |
| | .011 | .000 | .000 | .006 | .000 | .106 | .435 | .308 |
| X10 | -.096 | . | . | -.098 | . | .488 | .742 | .048 |
| | .396 | .000 | .000 | .394 | .000. | .076 | .007 | .448 |
| X11 | -.096 | . | . | -.098 | . | .488 | .742 | .048 |
| | .396 | .000 | .000 | .394 | .000 | .076 | .007 | .448 |

* * * * M U L T I P L E R E G R E S S I O N * * * *

| | X7 | X8 | X9 | X10 | X11 |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | .007 | .060 | .011 | .396 | .396 |
| ZZ1 | . | . | . | . | . |
| | .000 | .000 | .000 | .000 | .000 |
| Z1 | . | . | . | . | . |
| | .000 | .000 | .000 | .000 | .000 |
| Z2 | .594 | .333 | .749 | -.098 | -.098 |
| | .035 | .173 | .006 | .354 | .354 |
| Z3 | . | . | . | . | . |
| | .000 | .000 | .000 | .000 | .000 |
| X4 | .961 | .232 | .433 | .488 | .488 |
| | .000 | .260 | .106 | .076 | .076 |
| X5 | .502 | .282 | -.059 | .742 | .742 |
| | .069 | .215 | .435 | .007 | .007 |
| X6 | .357 | .000 | .181 | .048 | .048 |
| | .156 | .500 | .300 | .448 | .448 |
| X7 | 1.000 | .279 | .619 | .409 | .409 |
| | . | .217 | .028 | .120 | .120 |
| X8 | .279 | 1.000 | .134 | .163 | .163 |
| | .217 | . | .356 | .327 | .327 |
| X9 | .619 | .134 | 1.000 | -.026 | -.026 |
| | .028 | .356 | . | .471 | .471 |
| X10 | .409 | .163 | -.026 | 1.000 | 1.000 |
| | .120 | .327 | .471 | . | .000 |
| X11 | .409 | .163 | -.026 | 1.000 | 1.000 |
| | .120 | .327 | .471 | .000 | . |

* * * * M U L T I P L E R E G R E S S I O N * * * *

Equation Number 1 Dependent Variable.. ZV1

Descriptive Statistics are printed on Page 16

The following variables are constants or have missing correlations:

ZZ1 Z1 Z3

They will be deleted from the analysis.

Block Number 1. Method: Stepwise Criteria PIN .0500 POUT .1000

X8 X9 X10 X11

| Step | MultR | Rsq | F(Eqn) | SigF | | Variable | BetaIn |
|---|---|---|---|---|---|---|---|
| 1 | .7845 | .6154 | 12.800 | .007 | In: | X2 | -.7845 |
| 2 | .8998 | .8097 | 14.092 | .003 | In: | X5 | -.4424 |

Variable(s) Entered on Step Number
2.. X5

| | |
|---|---|
| Multiple R | .89983 |
| R Square | .80970 |
| Adjusted R Square | .75533 |
| Standard Error | 1.06345 |

Analysis of Variance

| | DF | Sum of Squares | Mean Square |
|---|---|---|---|
| Regression | 2 | 33.68345 | 16.84173 |
| Residual | 7 | 7.91655 | 1.13094 |

F = 14.89186 Signif F = .0030

---------- Variables in the Equation ----------

| Variable | B | SE B | Beta | T | Sig T |
|---|---|---|---|---|---|
| X2 | -3.352518 | .675003 | -.821854 | -4.967 | .0016 |
| X5 | -.381295 | .142620 | -.442393 | -2.673 | .0318 |
| (Constant) | 18.238849 | .569760 | | 32.011 | .0000 |

* * * * MULTIPLE REGRESSION * * * *

Equation Number 1 Dependent Variable.. SVI

---------- Variables not in the Equation ----------

| Variable | Beta In | Partial | Min Toler | T | Sig T |
|---|---|---|---|---|---|
| X4 | .006733 | .008808 | .325727 | .022 | .9835 |
| X6 | .214159 | .464303 | .094484 | 1.284 | .2465 |
| X7 | -.085601 | -.114272 | .339132 | -.282 | .7876 |
| X8 | -.157031 | -.320386 | .722166 | -.828 | .4391 |
| X9 | -.266094 | -.403872 | .426803 | -1.081 | .3211 |
| X10 | .340570 | .522403 | .447756 | 1.501 | .1841 |
| X11 | .340570 | .522403 | .447756 | 1.501 | .1841 |

End Block Number 1 PIN = .050 Limits reached.

* * * * MULTIPLE REGRESSION * * * *

* * * * M U L T I P L E  R E G R E S S I O N * * * *

Listwise Deletion of Missing Data

| | Mean | Std Devi | Label |
|---|---|---|---|
| Z5B | 2.133 | .594 | |
| ZZ1 | 1.000 | .000 | |
| Z1 | 1.000 | .000 | |
| Z2 | .500 | .527 | |
| Z3 | .000 | .000 | |
| X4 | 6.200 | 4.849 | |
| X5 | 2.000 | 2.494 | |
| X6 | 22.000 | 2.160 | |
| X7 | 30.500 | 6.916 | |
| X8 | .900 | .316 | |
| X9 | 1742.500 | 1951.642 | |
| X10 | .500 | 1.080 | |
| X11 | .500 | 1.080 | |

N of Cases = 10

* * * * M U L T I P L E  R E G R E S S I O N * * * *

Correlation, 1-tailed Sig:

' . ' is printed if a correlation cannot be computed.

| | Z5B | ZZ1 | Z1 | Z2 | Z3 | X4 | X5 | X6 |
|---|---|---|---|---|---|---|---|---|
| Z5B | 1.000 | . | . | -.355 | . | -.363 | .185 | -.352 |
| | . | .000 | .000 | .157 | .000 | .151 | .304 | .159 |
| ZZ1 | . | 1.000 | . | . | . | . | . | . |
| | .000 | . | .000 | .000 | .000 | .000 | .000 | .000 |
| Z1 | . | . | 1.000 | . | . | . | . | . |
| | .000 | .000 | . | .000 | .000 | .000 | .000 | .000 |
| Z2 | -.355 | . | . | 1.000 | . | .478 | -.085 | .293 |
| | .157 | .000 | .000 | . | .000 | .081 | .408 | .206 |
| Z3 | . | . | . | . | 1.000 | . | . | . |
| | .000 | .000 | .000 | .000 | . | .000 | .000 | .000 |
| X4 | -.363 | . | . | .478 | . | 1.000 | .625 | .318 |
| | .151 | .000 | .000 | .081 | .000 | . | .027 | .185 |
| X5 | .185 | . | . | -.085 | . | .625 | 1.000 | -.165 |
| | .304 | .000 | .000 | .408 | .000 | .027 | . | .324 |
| X6 | -.352 | . | . | .293 | . | .318 | -.165 | 1.000 |
| | .159 | .000 | .000 | .206 | .000 | .185 | .324 | . |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| X7 | -.449 | . | . | .594 | . | .961 | .502 | .357 |
| | .096 | .000 | .000 | .035 | .000 | .000 | .069 | .156 |
| X8 | .158 | . | . | .333 | . | .232 | .282 | .000 |
| | .332 | .000 | .000 | .173 | .000 | .260 | .215 | .500 |
| X9 | -.682 | . | . | .749 | . | .433 | -.059 | .181 |
| | .015 | .000 | .000 | .006 | .000 | .106 | .435 | .308 |
| X10 | -.023 | . | . | -.098 | . | .488 | .742 | .048 |
| | .475 | .000 | .000 | .394 | .000 | .076 | .007 | .448 |
| X11 | -.023 | . | . | -.098 | . | .488 | .742 | .048 |
| | .475 | .000 | .000 | .394 | .000 | .076 | .007 | .448 |

* * * * M U L T I P L E R E G R E S S I O N * * * *

| | X7 | X8 | X9 | X10 | X11 |
|---|---|---|---|---|---|
| ZSB | -.449 | .158 | -.682 | -.023 | -.023 |
| | .096 | .332 | .015 | .475 | .475 |
| ZZ1 | . | . | . | . | . |
| | .000 | .000 | .000 | .000 | .000 |
| Z1 | . | . | . | . | . |
| | .000 | .000 | .000 | .000 | .000 |
| Z2 | .594 | .333 | .749 | -.098 | -.098 |
| | .035 | .173 | .006 | .394 | .394 |
| Z3 | . | . | . | . | . |
| | .000 | .000 | .000 | .000 | .000 |
| X4 | .961 | .232 | .433 | .488 | .488 |
| | .000 | .260 | .106 | .076 | .076 |
| X5 | .502 | .282 | -.059 | .742 | .742 |
| | .069 | .215 | .435 | .007 | .007 |
| X6 | .357 | .000 | .181 | .048 | .048 |
| | .156 | .500 | .308 | .448 | .448 |
| X7 | 1.000 | .279 | .619 | .409 | .409 |
| | . | .217 | .028 | .120 | .120 |
| X8 | .279 | 1.000 | .134 | .163 | .163 |
| | .217 | . | .356 | .327 | .327 |
| X9 | .619 | .134 | 1.000 | -.026 | -.026 |
| | .028 | .356 | . | .471 | .471 |
| X10 | .409 | .163 | -.026 | 1.000 | 1.000 |
| | .120 | .327 | .471 | . | .000 |
| X11 | .409 | .163 | -.026 | 1.000 | 1.000 |
| | .120 | .327 | .471 | .000 | . |

Listwise Deletion of Missing Data

Equation Number 1  Dependent Variable..  Z5B

The following variables are constants or have missing correlations:

ZZ1  Z1  Z3

They will be deleted from the analysis.

Block Number 1.  Method: Stepwise  Criteria  FIN .0500  FOUT .1000

ZZ1  Z1  Z2  Z3  X6  X7  X8  X9
X4  X5  X10  X11

Variable(s) Entered on Step Number
1..  X9

| | |
|---|---|
| Multiple R | .68157 |
| R Square | .46453 |
| Adjusted R Square | .39760 |
| Standard Error | 6.91305 |

Analysis of Variance

| | DF | Sum of Squares | Mean Square |
|---|---|---|---|
| Regression | 1 | 331.67745 | 331.67745 |
| Residual | 8 | 382.32255 | 47.79032 |

F = 6.94026  Signif F = .0300

---------- Variables in the Equation ----------

| Variable | B | SE B | Beta | T | Sig T |
|---|---|---|---|---|---|
| X9 | -.003111 | .001181 | -.681567 | -2.634 | .0300 |
| (Constant) | 37.420125 | 3.001395 | | 12.465 | .0000 |

* * * *  M U L T I P L E  R E G R E S S I O N  * * * *

Equation Number 1  Dependent Variable..  Z5B

---------- Variables not in the Equation ----------

| Variable | Beta In | Partial | Min Toler | T | Sig T |
|---|---|---|---|---|---|
| Z2 | .355216 | .321413 | .438405 | .898 | .3990 |
| X6 | -.236609 | -.318001 | .967219 | -.887 | .4043 |
| X7 | -.044056 | -.047280 | .616729 | -.125 | .9039 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| X7 | -.449 | . | . | .594 | . | .961 | .502 | .357 |
| | .096 | .000 | .000 | .035 | .000 | .000 | .069 | .156 |
| X8 | .158 | . | . | .333 | . | .232 | .282 | .000 |
| | .332 | .000 | .000 | .173 | .000 | .260 | .215 | .500 |
| X9 | -.682 | . | . | .749 | . | .433 | -.059 | .181 |
| | .015 | .000 | .000 | .006 | .000 | .106 | .435 | .308 |
| X10 | -.023 | . | . | -.098 | . | .488 | .742 | .048 |
| | .475 | .000 | .000 | .394 | .000 | .076 | .007 | .448 |
| X11 | -.023 | . | . | -.098 | . | .488 | .742 | .048 |
| | .475 | .000 | .000 | .394 | .000 | .076 | .007 | .448 |

* * * * M U L T I P L E R E G R E S S I O N * * * *

| | X7 | X8 | X9 | X10 | X11 |
|---|---|---|---|---|---|
| ZSB | -.449 | .158 | -.682 | -.023 | -.023 |
| | .096 | .332 | .015 | .475 | .475 |
| ZZ1 | . | . | . | . | . |
| | .000 | .000 | .000 | .000 | .000 |
| Z1 | . | . | . | . | . |
| | .000 | .000 | .000 | .000 | .000 |
| Z2 | .594 | .333 | .749 | -.098 | -.098 |
| | .035 | .173 | .006 | .394 | .394 |
| Z3 | . | . | . | . | . |
| | .000 | .000 | .000 | .000 | .000 |
| X4 | .961 | .232 | .433 | .488 | .488 |
| | .000 | .260 | .106 | .076 | .076 |
| X5 | .502 | .282 | -.059 | .742 | .742 |
| | .069 | .215 | .435 | .007 | .007 |
| X6 | .357 | .000 | .181 | .048 | .048 |
| | .156 | .500 | .308 | .448 | .448 |
| X7 | 1.000 | .279 | .619 | .409 | .409 |
| | . | .217 | .028 | .120 | .120 |
| X8 | .279 | 1.000 | .134 | .163 | .163 |
| | .217 | . | .356 | .327 | .327 |
| X9 | .619 | .134 | 1.000 | -.026 | -.026 |
| | .028 | .356 | . | .471 | .471 |
| X10 | .409 | .163 | -.026 | 1.000 | 1.000 |
| | .120 | .327 | .471 | . | .000 |
| X11 | .409 | .163 | -.026 | 1.000 | 1.000 |
| | .120 | .327 | .471 | .000 | . |

| | | | | | |
|---|---|---|---|---|---|
| X4 | -.083313 | -.102632 | .912592 | -.273 | .7927 |
| X5 | .145027 | .197840 | .996465 | .534 | .6039 |
| X10 | -.041180 | -.056255 | .999298 | -.149 | .8857 |
| X11 | -.041180 | -.056255 | .999298 | -.149 | .8857 |

End Block Number 1 PIN = .050 Limits reached.

* * * * M U L T I P L E R E G R E S S I O N * * * *

Listwise Deletion of Missing Data

| | Mean | Std Devi | Label |
|---|---|---|---|
| ZSA | 38.800 | 5.245 | |
| ZS1 | 1.000 | .000 | |
| Z1 | 1.000 | .000 | |
| Z2 | .500 | .527 | |
| Z3 | .000 | .000 | |
| X4 | 6.200 | 4.033 | |
| X5 | 2.000 | 2.494 | |
| X6 | 22.000 | 2.160 | |
| X7 | 30.500 | 6.316 | |
| X8 | .900 | .316 | |
| X9 | 1742.500 | 1951.642 | |
| X10 | .500 | 1.080 | |
| X11 | .500 | 1.080 | |

N of Cases = 10

* * * * M U L T I P L E R E G R E S S I O N * * * *

Correlation, 1-tailed Sig:

' . ' is printed if a correlation cannot be computed.

| | ZSA | ZS1 | Z1 | Z2 | Z3 | X4 | X5 | X6 |
|---|---|---|---|---|---|---|---|---|
| ZSA | 1.000 | | | 563 | | .408 | .025 | .029 |
| | . | .090 | .009 | .045 | .000 | .121 | .472 | .468 |

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| ZZ1 | . | 1.000 | . | . | . | . | . | . |
| | .000 | . | .000 | .000 | .000 | .000 | .000 | .000 |
| Z1 | . | . | 1.000 | . | . | . | . | . |
| | .000 | .000 | | .000 | .000 | .000 | .000 | .000 |
| Z2 | .563 | . | . | 1.000 | . | .478 | -.085 | .293 |
| | .045 | .000 | .000 | | .000 | .021 | .108 | .206 |
| Z3 | . | . | . | . | 1.000 | . | . | . |
| | .000 | .000 | .000 | .000 | | .000 | .000 | .000 |
| X4 | .408 | . | . | .479 | . | 1.000 | .625 | .318 |
| | .121 | .000 | .000 | .081 | .000 | . | .027 | .185 |
| X5 | .025 | . | . | -.085 | . | .625 | 1.000 | -.165 |
| | .472 | .000 | .000 | .408 | .000 | .027 | . | .324 |
| X6 | .029 | . | . | .293 | . | .318 | -.165 | 1.000 |
| | .468 | .000 | .000 | .206 | .000 | .185 | .324 | . |
| X7 | .606 | . | . | .594 | . | .961 | .502 | .357 |
| | .032 | .000 | .000 | .035 | .000 | .000 | .069 | .156 |
| X8 | .255 | . | . | .333 | . | .232 | .282 | .000 |
| | .239 | .000 | .000 | .173 | .000 | .260 | .215 | .500 |
| X9 | .722 | . | . | .749 | . | .433 | -.059 | .181 |
| | .009 | .000 | .000 | .006 | .000 | .106 | .435 | .308 |
| X10 | .098 | . | . | -.098 | . | .488 | .742 | .048 |
| | .394 | .000 | .000 | .394 | .000 | .076 | .007 | .448 |
| X11 | .098 | . | . | -.098 | . | .488 | .742 | .048 |
| | .394 | .000 | .000 | .394 | .000 | .076 | .007 | .448 |

* * * * M U L T I P L E R E G R E S S I O N * * * *

| | X7 | X8 | X9 | X10 | X11 |
|---|---|---|---|---|---|
| Z5A | .606 | .255 | .722 | .098 | .098 |
| | .032 | .239 | .009 | .394 | .394 |
| ZZ1 | . | . | . | . | . |
| | .000 | .000 | .000 | .000 | .000 |
| Z1 | . | . | . | . | . |
| | .000 | .000 | .000 | .000 | .000 |
| Z2 | .594 | .333 | .749 | -.098 | -.098 |
| | .035 | .173 | .006 | .394 | .394 |

| | | | | | |
|---|---|---|---|---|---|
| Z3 | . | . | . | . | . |
| | .000 | .000 | .000 | .000 | .000 |
| X4 | .961 | .232 | .433 | .488 | .488 |
| | .000 | .260 | .106 | .076 | .076 |
| X5 | .502 | .282 | -.059 | .742 | .742 |
| | .069 | .215 | .435 | .007 | .007 |
| X6 | .357 | .000 | .181 | .048 | .048 |
| | .156 | .500 | .308 | .448 | .448 |
| X7 | 1.000 | .279 | .619 | .409 | .409 |
| | . | .217 | .028 | .120 | .120 |
| X8 | .279 | 1.000 | .134 | .163 | .163 |
| | .217 | . | .356 | .327 | .327 |
| X9 | .619 | .134 | 1.000 | -.026 | -.026 |
| | .028 | .356 | . | .471 | .471 |
| X10 | .409 | .163 | -.026 | 1.000 | 1.000 |
| | .120 | .327 | .471 | . | .000 |
| X11 | .409 | .163 | -.026 | 1.000 | 1.000 |
| | .120 | .327 | .471 | .000 | . |

* * * * M U L T I P L E R E G R E S S I O N * * * *

Equation Number 1 Dependent Variable.. Z5A

Descriptive Statistics are printed on Page 31

The following variables are constants or have missing correlations:

ZZ1 Z1 Z3

They will be deleted from the analysis.

Block Number 1. Method: Stepwise Criteria FIN .0500 POUT .1000

ZZ1 Z1 Z2 Z3 X4 X5 X6 X7
X8 X9 X10 X11

| Step | MultR | Rsq | F(Eqn) | SigF | | Variable | BetaIn |
|---|---|---|---|---|---|---|---|
| 1 | .7220 | .5213 | 8.713 | .018 | In: | X9 | .7220 |

Variable(s) Entered on Step Number
1.. X9

| | |
|---|---|
| Multiple R | .72203 |
| R Square | .52133 |
| Adjusted R Square | .46149 |
| Standard Error | 3.84901 |

Analysis of Variance

| | DF | Sum of Squares | Mean Square |
|---|---|---|---|
| Regression | 1 | 129.08079 | 129.08079 |
| Residual | 8 | 118.51921 | 14.81490 |

F = 8.71290 Signif F = .0184

---------- Variables in the Equation ----------

| Variable | B | SE B | Beta | T | Sig T |
|---|---|---|---|---|---|
| X9 | .001940 | 6.574E-04 | .722030 | 2.952 | .0184 |
| (Constant) | 35.418712 | 1.671435 | | 21.191 | .0000 |

* * * * M U L T I P L E R E G R E S S I O N * * * *

Equation Number 1 Dependent Variable.. Z5A

---------- Variables not in the Equation ----------

| Variable | Beta In | Partial | Min Toler | T | Sig T |
|---|---|---|---|---|---|
| X2 | .049316 | .047197 | .438405 | .125 | .9040 |
| X4 | .117499 | .153092 | .812592 | .410 | .6942 |
| X5 | .060649 | .099048 | .996465 | .263 | .7999 |
| X6 | -.104742 | -.148890 | .967219 | -.398 | .7022 |
| X7 | .258550 | .293486 | .616729 | .812 | .4434 |
| X8 | .160915 | .230496 | .982131 | .627 | .5507 |
| X10 | .117268 | .169437 | .999298 | .455 | .6630 |
| X11 | .117268 | .169437 | .999298 | .455 | .6630 |

End Block Number 1 PIN = .050 Limits reached.

# BIBLIOGRAPHY


- Ball, L. & R. Harris, "SMIS Member: A Membership Analysis", MIS Quarterly, Vol. 6, No. 1, March 1982.

- Bloombecker, J., "Short- Circuiting Computer Crime", Datamation, Vol. 11, No. 6, October 1, 1989, p.p. 71-72.

- Boockholdt, J.L., "Computers/Technology: Protecting mainframe data from PCs", Journal of Accountancy, Vol. 8, No. 4, April 1991.

- Brancheau, J.C. & J.C. Wetherbe, "Key Issues in Information System Management", MIS Quarterly, Vol. 12, No. 2, March 1987.

- Carter, R., "Dependence and Disaster: Recovering from EDP Systems Failure", Management Services, UK, VoL. 32, No. 12, Dec. 1988.

- Cockford, N., An Introduction To Risk Management, Cambridge: Woodhead, Faulkner Ltd., 1980.

- Cooper, James Arlin, Computer and Communications Security: Strategies for the 1990s, N.Y: Mc Graw- Hill Book Company, 1989.

- Ernest & Whinney, "Concern about Computer Security Increasing", Journal of Accountancy, Vol. 18, No. 3, June 1987.

- Farhoomand, Ali F., "Managing Computer Security", Datamation, Vol. 10, No. 5, January 1, 1989.

• Hartog, C. & M. Herbert, "1985 opinion Survey of MIS Managers: Key Issues", MIS Quarterly, Vol.10, No. 4, December 1986.

• Igbaria, Magid et al., "Microcomputer Applications", Information & Management, Vol. 16, 1989.

• Kwan, Stephen K. & Kathleen Curley, "corporate MIS/DP and End User Computing: The Emergence of a New Partneship", Database, Summer 1989.

• Laudon, Kenneth C. & Jane Price Laudon, Management Information Systems, N.Y: Macmillan Publishing Company, 1991.

• Loch, Karen, Houston Carr. & Merill E. Warlentein, "Threats to Information Systems: Today's Reality, Yesterday's Understanding", MIS Quarterly, Vol. 16, No. 2, June 1992.

• Mansour, Ali H. & Hugh J. Watson, "The Determinants of Computer Based Information System Performance", Academy of Management Journal, Vol. 23, No. 3, 1980.

• Markus, M. Lynn & Neils Andersen, "Power Over Users: Its Exercise by System Professional", Communication of the ACM, Vol. 30, No. 6, June 1987.

• Meall, L., "Survival of the Fittest"' Accountancy, UK, Vol. 103, No. 1147, March 1989.

• National Research Council, Computers at Risk, National Academy Press, Washington, DC, 1991.

- Neiderman, F., J.C. Brancheau, & J.C. Wetherbe," Information Systems Management Issues of the 1990s", MIS Quarterly, Vol. 15, No. 4, December 1991.

- Nelson, R. & P. Cheney, "Training End Users: An Exploratory Study", MIS Quarterly, Vol. 11, No. 4, December 1987.

- Parker, Charles S., Management Information Systems, N.Y: Mc Graw-Hill Publishing Company, 1989.

- Sprage, Ralph H. & B.C. McNurlin, Information Systems in Practice, New Jersey: Prentice-Hall, Inc., 1986.

- Srinivasan, Ananth, "Alternative Measures of System Effectiveness", MIS Quarterly, Vol. 9, No. 3, September 1985.

- Szuprowicz, B.O., "Technological Vulnerability: How Serious a Threat to your Business?", Canadian Datasystem, Vol. 20, No. 10, October 1988.

- Terry, George R., Principles of Management, London: IRWI- DORSEY INTERNATIONAL, 1972.

- Thierauf, Robert J., Effective Management Information Systems, Ohio: Bell & Howell Company, 1984.

- Yaverbaum, Gayle J., "Critical Factors in the User Environment", MIS Quarterly, Vol. 12, No. 1, March 1988.