INVESTIGATING THE PERCEIVED THREATS OF COMPUTERIZED ACCOUNTING INFORMATION SYSTEMS IN DEVELOPING COUNTRIES: AN EMPIRICAL STUDY ON SAUDI ORGANIZATIONS

Dr. Ahmad A. Abu-Musa*
Accounting & Management Information Systems
King Fadh University of Petroleum & Minerals
Dhahran, Saudi Arabia

ABSTRACT

The objective of this paper is to investigate the significant perceived security threats of computerized accounting information systems (CAIS) in Saudi organizations. An empirical survey using a self administered questionnaire has been carried out to achieve this objective. The survey results revealed that almost half of the responded Saudi organizations have suffered financial losses due to internal and external CAIS security breaches. The statistical results also revealed that accidental and intentional entry of bad data; accidental destruction of data by employees; employees' sharing of passwords; introduction of computer viruses to CAIS; suppression and destruction of output; unauthorized document visibility; and directing prints and distributed information to people who are not entitled to receive are the most significant perceived security threats to CAIS in Saudi organizations. Accordingly, it is recommended to strengthen the security controls over the above weaken security areas and to enhance the awareness of CAIS security issues among Saudi organizations to achieve better protection to their CAIS.

Key Words: Perceived Security Threats; Information Technology; Accounting Information Systems; Saudi Organizations; Empirical Survey

INTRODUCTION

The rapid change in information technology, the wide spread of user-friendly systems and the great desire of organisations to acquire and implement up-to-date computerised systems and software have made computers much easier to be used and enabled accounting tasks to be accomplished much faster and accurate than hitherto. On the other hand, this advanced technology has also created significant risks related to ensuring the security and integrity of CAIS. The technology, in many cases, has been developed faster than the advancement in control practices and has not been combined with similar development of the employees' knowledge, skills, awareness, and compliance. Every day, reports can be found in accounting and financial publications about computer related data errors, incorrect financial information, violation of internal controls, thefts, burglaries, fires and sabotage. Organizations should be aware with the potential security threats that might challenge their CAIS and implement the relevant security controls to prevent, detect and correct such security breaches. Although considerable efforts have been made by practising accountants to reduce the vulnerability of

---

* Dr Ahmad A. Abu-Musa is an Assistant Professor at Accounting Department, Faculty of Commerce, Tanta University, Egypt. Currently, Dr. Abu-Musa is a Visiting Assistant Professor at the Department of Accounting & Management Information Systems, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia.

Acknowledgement: The author acknowledges the financial support of the College of Industrial Management, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia.

CAIS to such events, it is argued that an increased effort is still required (Abu-Musa, 2001 and 2003).

The objective of this paper is to investigate the perceived security threats of CAIS in Saudi organizations using a proposed security threats checklist. The security threats checklist of CAIS was developed based on the available literature and the empirical results of previous studies in that area. This research is a trial to answer the following research questions:

1. What are the most important perceived security threats challenging CAIS in the Saudi organizations?

2. Are there significant differences among different types of Saudi organizations regarding the perceived security threats challenging their CAIS?

The remainder of this paper is organized as follows. The next section presents the literature review and pervious studies related to the perceived threats of CAIS. The study's research method is then described. This is followed by the statement of research hypothesis and a presentation of the study's major empirical results. The final section of this paper provides the research's major conclusion and recommendations for further research.

LITERATURE REVIEW

Reviewing the literature concerned with evaluating the security of computerised information systems reveals the paucity of available studies in that particular area of research. One reason is that the security of CAIS is a relatively new research area. The main objectives of previous studies under this category have been to list the security threats that might threaten computerised information systems in an organisation; to explore the significance of such perceived security threats in the real world; and to investigate their occurrence and potential losses in different organisations.

One of the most important studies in this area was carried out by Loch et al. (1992). The researchers conducted a survey to explore the perception of Management Information Systems (MIS) Executives regarding the security threats in microcomputer, mainframe computer, and network environments. The study addressed two main questions to be investigated: What are the threats to information systems and resident data? And; which of these are the most serious threats?

Loch et al. (1992) developed a list of twelve security threats, derived from the available literature, to be empirically examined in that study. These security threats are:

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. Unauthorised access to data/system by employees
6. Inadequate control over media (disks and tapes)
7. Poor control over manual handling on input/ output
8. Access to data/ system by outsiders (hackers)
9. Access to data/ system by outsiders (competitors)
10. Entry into system of computer viruses and worms
11. Weak, ineffective, or inadequate physical control
12. Natural disaster: fire, flood, loss of power, communications.

Loch et al. (1992) piloted their proposed questionnaire; then an empirical survey was conducted by sending the final developed questionnaire to 657 senior MIS managers in the US. The respondents were asked to rank the top three threats from a given security threats list for each information systems environment. After conducting a follow up mailing, they managed to obtain a 20 percent response rate. The study used three methods of data analysis (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 computerised systems. The results of the study indicated that natural disasters and employee accidental actions were ranked among the top threats by all three methods. External threats received 37 percent of the weighted votes and internal threats received 62.4 percent of the weighted votes, giving internal threats an almost 2 to 1 value over external. These results confirmed the experts' claims that the greatest threats come from inside organisations. The results of that study also revealed that accidental destruction of data by employees, accidental entry of bad data by employees and inadequate control over media were perceived as the most important perceived threats in a microcomputer environment. The most important three threats to mainframe computers were accidental entry of bad data by employees, natural disasters and then accidental destruction of data by employees. Natural disasters, access to systems by hackers and weak / ineffective controls were the main threats in the network environment.

From the researcher's point of view, the Loch et al. security threats list included some elements which could not be properly considered security threats. Loch et al. included the lack or inadequacy of some security controls (such as inadequate control over media (disks and tapes); poor control over manual handling on input / output; and weak physical controls) as security threats. This is confusion: weak policing does not itself create the crime. However, a selected number of precise security threats as used in Loch et al. were included in the questionnaire to be examined here in the Saudi environment. Other variables (inadequate control over media; poor control over manual handling on input / output; and weak physical controls) were excluded from the adopted security threats list. Moreover, a number of threats that are untested in Loch et al were included to be tested in Saudi environment.

Since accounting information system security has become one of the major concerns for information systems' auditors, Davis (1996) tried to discover the current status of the security issues in practice. Davis conducted a survey on a random sample of the members of Information Systems Audit and Control Association (ISACA) and the American Institute of Certified Public Accountants (AICPA). The respondents were sent a copy of the questionnaire, "Threats to Accounting Information Systems Security Survey" which was adapted from Loch et al. (1992), in replication of their work.

The results of Davis' survey (1996) indicated that 95 percent of the respondents felt that there is at least a moderate level of overall risk to CAIS security. Moreover, information systems auditors recognised that different computing environments have different relative levels of security risks. The results showed that a system of microcomputers with connections to an external network was viewed as the highest risk environment, while a mainframe environment was viewed as having the lowest threat level.

Employees' accidental entry of "bad" data and the accidental destruction of data, as well as the introduction of computer viruses, were considered to be the three top threats in a microcomputer environment. However, unauthorized access to data and/or system by employees, accidental entry of "bad" data by employees and poor segregation of information system duties were rated as the major threats to the minicomputer environment. Concerning

the mainframe computer environment, accidental entry of "bad" data by employees, natural disaster, and unauthorized access to data and/or system by employees were perceived as the main threats, while unauthorized access to data and/or system by both outsider (hackers) and insiders (employees), and technology advances faster than control practice were said to be the most important threats in network computer environment. The following table represents a comparative summary of the security threats in the different computer environments:

Security Threats	Microcomputer Environment (Total Votes)	Minicomputer Environment (Total Votes)	Mainframe Computer Environment (Total Votes)	Network Computer Environment (Total Votes)
1. Accidental entry of "bad" data by employees	38	31	42	25
2. Intentional entry of "bad" data by employees	5	7	9	5
3. Accidental destruction of data by employees	42	16	18	19
4. Intentional destruction of data by employees	2	1	5	1
5.Unauthorized access to data / system by employees	27	34	31	33
6. Inadequate control over storage media (i.e. disks, tapes, diskettes)	32	16	9	6
7. Poor control over manual handling of input and output data	11	15	23	7
8.Unauthorized access to data / system by outsider (hackers)	8	17	22	51
9.Introduction of computer viruses to systems	41	11	4	28
10.Weak (ineffective, inadequate) physical access controls permitting unauthorized access to systems	27	15	6	14
11. Natural disaster such as fire, flooding, loss of power	3	17	35	17
12.Poor segregation of information systems duties (e.g. programming and operations)	16	31	28	8
13..Poor segregation of accounting duties (i.e. authorisation, recording, and custody)	17	23	20	12
14.Employees sharing passwords	9	17	25	16
15.Interception of data transmissions from remote locations	1	4	7	19
16. Technology advances faster than control practices	20	11	10	48
17. Others	1	3	6	0

(Table 1: The Results of Davis' Survey, 1996; Source: Adapted from Davis 1996)

Again, one of the main criticisms of Davis' study is its treatment of some inadequate or ineffective security controls as security threats. For example, Davis included as "threats" factors such as inadequate control over storage media; poor control over manual handling of input and output data; weak or inadequate physical access control permitting unauthorized access to systems; poor segregation of information systems duties; poor segregation of accounting duties; and employees sharing passwords. Again, attempting to distinguish

between security threats and inadequate security controls, the current research has excluded all of the above prospective security controls from the proposed security threats list. The other security threats examined in Davis study were included within the present research's security threat list, to be reinvestigated in the Saudi environment.

Recently, client / server computing become a serious alternative to mainframe computing in many organisations. Although the client / server computing system offers some benefits, it is also exposes the computing environment to additional risks: the flexibility that makes it attractive could also make it more vulnerable to security threats. Ryan and Bordoloi's (1997) research explored how companies moving from a mainframe to a client / server environment evaluated and took security measures to protect against potential security threats. The purpose of the Ryan and Bordoloi (1997) study was to explore the following three research questions:

- Is the seriousness of a potential security threat perceived differently in the client / server and mainframe environment?
- Is the degree of preparation against a potential security threat different in the two environments?
- For each of the two environments, are measures taken to prepare against a potential threat commensurate with its perceived seriousness?

Based on a literature review and on information acquired from several industry consultants, Ryan and Bordoloi developed the following list of fifteen security threats:

1. Access to data / system by outsiders (hackers, etc.).
2. Accidental destruction of data by employees.
3. Accidental entry of erroneous data by employees.
4. Inadequate audit trial.
5. Inadequate or non-existence logon procedures.
6. Intentional destruction of data by employees.
7. Intentional entry of erroneous data by employees.
8. Loss due to inadequate backups or log files.
9. Natural disaster: fire, flood, loss of power, etc.
10. Sharing passwords.
11. Single point of Failure.
12. Uncontrolled read and / or updates access.
13. Uncontrolled user privilege.
14. Viruses, bombs or worms.
15. Weak / ineffective or inadequate physical control.

A questionnaire was designed incorporating the above security threats, and distributed to the attendees of client / server sessions at an industry technical conference. The conference's attendees were information systems technical professionals from medium and large corporations. One hundred and twenty questionnaires were distributed. 52 usable questionnaires were returned, which represented a 47 percent response rate. The respondents were asked to rate the seriousness of the 15 potential security threats to their companies, in both of mainframe and client / server environments. A scale rating from 1 to 10 was used; where a rating 1 meant that the potential threat was not a concern to the company; and a rating of 10 meant that the threat was a very critical concern. The respondents were also asked to rate the degree to which their company had taken control measures to protect against

potential risks in each of the two environments. Again, a 10-point scale was used, where a rating of 1 meant that no measures were taken against a potential threat; and a rating of 10 meant that all possible measures were taken

The results of the study indicated that the average ratings of 7 out of the 15 potential security threats were significantly different ($p = 0.05$) for the two computing environments. In each of these cases, the perceived risk was rated higher in the mainframe environment. These seven significant security threats were:

- Accidental destruction of data by employees
- Accidental entry of erroneous data by employees
- Intentional destruction of data by employees
- Intentional entry of erroneous data by employees
- Loss due to inadequate backups or log files
- Natural disaster: fire, flood, loss of power, etc.
- Single point of failure.

The results of the study also indicated that companies were less prepared and had taken fewer measures to protect against potential security threats in client / server environments when compared with mainframe environments. For every threat listed, there was a significant difference in the ratings of preparedness for the mainframe versus the client / server environment. Further, the mean rating for the client / server environment was lower than that for the mainframe environment.

Again, it seems that Ryan and Bordoloi (1997) did not always clearly distinguish between security threats and the inadequacy of security controls. They treated many inadequate security controls as security threats (such as inadequate audit trial, the inadequate or non-existence log-on procedures, loss due to inadequate backups or log files, sharing passwords, uncontrolled read and / or update access, uncontrolled user privilege, and weak / ineffective or inadequate physical controls). However, Ryan and Bordoloi (1997) acknowledged that some of the items might not be considered security threats in the strict sense of the term; nevertheless, they argued, they might matter very much to the continued existence of the organisation. The researchers therefore included them in their survey and reported them as important to good information technology management and practice (p. 139). In this research, security threats and controls have been carefully distinguished. Therefore, eight security threats mentioned in Ryan and Bordoloi's study were considered and included in the security threat list to be investigated in the Saudi environment.

Computerised accounting systems have become more readily available to all types and sizes of businesses. Henry (1997) conducted a survey on 261 companies in Hampton Roads, Virginia, USA, to determine the nature of their accounting systems and security in use. He attempted to ascertain the degree of correspondence between the theory and actual practice. Seven basic security methods for computerised accounting information systems were discussed and presented in his survey. These methods included encryption, password access, backup of data, virus protection, and authorisation for system changes, physical system security, and periodic audits. The results of Henry's survey indicated that 80.3 percent of the companies backed-up their accounting systems. 74.4 percent of the companies secured their accounting system with passwords, but only 42.7 percent utilised protection from viruses. Physical security and authorisation for changes to the system were employed by less than 40 percent of the respondents. The survey results also showed that only 15 companies used encryption for their accounting data, which was a surprising result, considering the number of

companies utilising some form of communication hardware. Almost 45 percent of the sample underwent some sort of audit of their accounting data.

In a further, recent study on the banking sector, Abu-Musa (2001) carried out a survey to investigate the significant perceived security threats to CAIS in the Egyptian banking industry. A self-administered questionnaire has been used to investigate the opinions of the heads of internal audit departments (HoIAD) and the heads of computer departments (HoCD), in the entire population (sixty-six banks' headquarters) of the Egyptian banking industry (EBI), regarding the perceived security threats to their CAIS. Two copies of the questionnaire were directed to each individual bank's headquarters. One was given to the head of the computer department and the other to the head of the internal audit department. Seventy-nine completed and usable questionnaires were collected from forty-six different banks' headquarters. Forty-six of these questionnaires were completed by the HoCD, and thirty-three questionnaires were filled by the HoIAD. The response rate of the computers departments (after excluding merged, liquidated, too distant, and non computerised banks) was 79.3%, whilst the response rate was 56.9% from the internal audit departments. Response was controlled by personal administration and collection by the researcher, minimising respondent bias.

Abu-Musa (2001) developed the following list of nineteen security threats to be used in investigating the perceived security threats of CAIS in the EBI:

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 the data and / or system by employees
6. Unauthorized access to the data and / or system by outsiders (hackers)
7. Employees' sharing of passwords
8. Natural disaster such as fire, flooding, loss of power
9. Human- made disasters such as fire, loss of power
10. Introduction (entry) of computer viruses to the system
11. Suppression or destruction of output
12. Creation of fictitious / incorrect output
13. Theft of data / information
14. Unauthorized copying of output
15. Unauthorized document visibility by displaying on monitors or printed on paper
16. Printing and distributing of information by unauthorized persons.
17. Prints and distributed information are directed to people who are not entitled to receive it.
18. Sensitive documents are handed to non- security cleared personnel for shredding.
19. Interception of data transmissions from remote locations

The above list of CAIS security threats was derived from previous studies (Loch et al., 1992; Davis, 1996 and 1997; FFIEC, 1996; and Henry, 1997) and from the available literature in this area. However, some suggested security threats were included in this list to be investigated for the first time (for example, threats numbers 9, 11, 12, 13, 14, 15, 16, 17, 18, and 19) in that study.

Abu-Musa (2001) used a suggested five-scale security threats list (less than once a year, once a year to monthly, once a month to weekly, once a week to daily, and daily or more frequently) to investigate the importance and the materiality of CAIS security threats through

their frequency of occurrence. The respondents were asked to scale the occurrence frequency of each security threat in their banks. The main concern was to investigate the frequency of occurrence of each security threat - as a proxy for its materiality, importance, or risks - regardless of the prospective value of financial losses occurred. It is argued that an occurrence of a threat x might cost the bank only a few pounds in some cases, could cost it several millions or billions in other cases, while in the worst cases, it could lead the bank into bankruptcy.

The statistical results of the empirical study revealed that accidental entry of bad data by employees, accidental destruction of data by employees, introduction of computer viruses to the system, natural and human-made disasters, employees' sharing of passwords and misdirecting prints and distributing information to people not entitled to receive them are the most perceived significant security threats to CAIS in the EBI. In all these cases, the heads of internal audit departments (HoIAD) reported higher rank of frequencies of occurrence of CAIS security threats compared with the heads of computer departments (HoCD). Except for the unauthorized access to data or/and CAIS by outsiders (hackers), the statistical results show no significant differences of the perceived security threats among different bank types. The CAIS security threats list suggested by Abu-Musa (2001) will be adopted and used in this research to investigate the significant perceived security threats challenging CAIS is Saudi environment.

THE RESEARCH HYPOTHESES

The current research is an attempt to investigate the following research hypotheses:

1. There are significant differences among different Saudi organizations concerned with the perceived security threats challenging their CAIS.
2. There are significant differences in the opinions of different respondent groups regarding the perceived security threats of CAIS in Saudi organizations.

THE RESEARCH METHODOLOGY

In this research an empirical survey has been conducted to investigate the significant perceived CAIS security threats Saudi environment. A self- administered questionnaire (see: appendix 1) has been used to collect the data needed to investigate and test the research hypotheses. The survey approach, using a self-administered questionnaire, seems to be the most appropriate approach for conducting this research. One of the main strengths of the survey approach is its ability to collect data from a large number of organizations, located in a spread of locations. Moreover, this could allow the researcher to implement quantitative analysis to test the research hypotheses and also gives the potential opportunity to generalize the research findings.

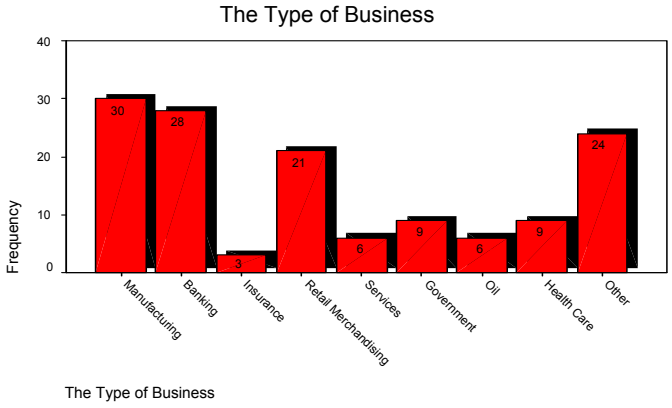
Selecting a representative, accurate and unbiased research sample is an important step towards the survey's success. Random selection of the individual observations of the research sample is a significant way to obtain an accurate and a representative sample. In this research, four hundreds questionnaires have been randomly distributed to different types of Saudi organizations (Manufacturing companies. Banks. Insurance companies, retail merchandising, Oil and Gas companies, Services companies, Heath Care, Government units and others) in the seven Saudi cities: Riyadh, Jeddah, Dhahran, Dammam, Thuqba, Khubar, and Jubail. After the following up, two-hundreds and eight questionnaires; representing fifty-two percent

initial response rate; had been collected. However, 38 questionnaires of the collected questionnaires, where only manual accounting systems were used, have been excluded form the analysis. Another 34 incomplete questionnaires had not been considered in the data analysis. The respondents of the previous organizations refused to complete the questionnaires; claiming that it is sensitive and confidential information. After excluding the incomplete and invalid responses, the research ended with 136 valid and usable questionnaires, representing 34 percent response rate. This response rate is considered as a high response rate in such kind of empirical surveys.

The collected data has been analyzed using the statistical package for social sciences (SPSS) version 12. Descriptive statistics (such as frequencies and percentages) of the collected data had been carried out to recognize the main characteristics of the research variables. In addition, non-parametric tests (such as the Kruskal-Wallis test and ANOVA test) had been used to investigate and test the research hypotheses. In the next section a brief description of the research sample and the respondents profile will be presented; and the main research findings will be discussed.

THE RESEARCH RESULTS

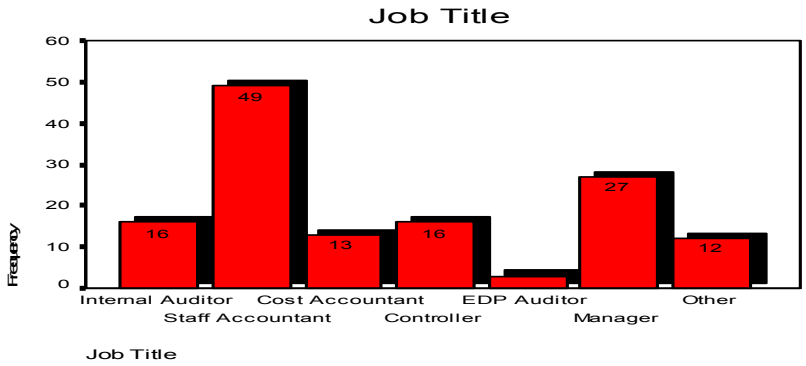
The research has a representative and unbiased research sample. One hundred and four valid and usable questionnaires were randomly selected from a wide range of Saudi organizations. The selected sample is quite representative of the population from which it was drawn (figure 1). It is observed that thirty of the responded organizations were manufacturing companies; and twenty-eight were banks: representing 22.1 percent and 20.6 percent of the total responses respectively. Twenty-one respondents from retail merchandising - representing 15.4 percent of the total response - participated in the survey. Nine respondents in each of the categories of governmental units and health care organizations have responded: representing 6.6 percent each of the total sample. Moreover, 6 respondents in each of the categories of services organizations and oil and Gas industry participated in the current survey. In addition, three respondents, representing 2.2 percent of the total were belonged to insurance companies. Twenty-four other organizations (17.6 percent of the total) participated in this survey were hotels; car rental organizations, Décor and carpentry firms; Publishing and printing organizations; Accounting and auditing firms; Construction companies; and Design organizations.



(Figure 1: Responded Businesses)

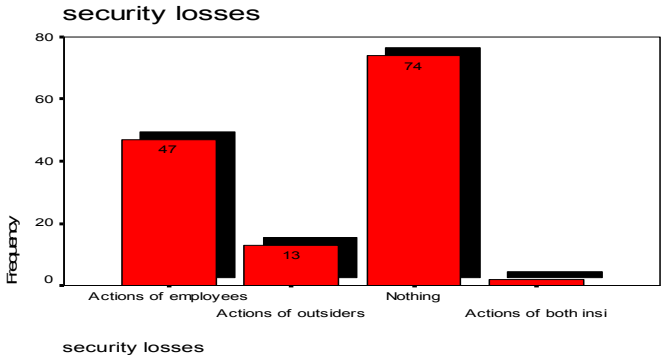
Top

As figure 2 shows forty-nine of the respondents (36 percent) were staff accountant; 27 respondents (approximately 20 percent) were managers; 16 respondents (approximately 12 percent) were internal auditors and a similar number of the respondents were controllers. Moreover, 13 respondents were working as cost accountants and three respondents were EDP auditors. Again, the respondents seem to be quite representative to the job structure in Saudi organizations (figure 2).



(Figure 2: Respondents' Job Titles)

The statistical results revealed that forty-seven of the respondents, representing 34.6 of the total respondents reported suffering from internal financial security losses as a result of employees' dishonest actions (figure 3). Thirteen respondents (9.6 percent) reported that they had suffered from external security losses due to some hacking actions outside their organizations; and only two respondents reported suffering security losses due to both internal and external security breaches during the last twelve months. It is observed that merely half of the respondents reported security financial losses. The reported security losses ranged form SR10, 000 in some organizations to more than 200 millions in some financial institutions. Reporting of losses may be a sensitive and potentially unreliable data item in this questionnaire research. Many organizations were reluctant to report such security to maintain their reputation.



(Figure 3: Security Financial Losses)

The statistical findings related to the perceived security threats challenging CAIS in Saudi organizations will now be presented and discussed in the following sections.

Accidental Entry of Bad Data by Employees

Respondents were asked to indicate the occurrence frequency of accidental entry of bad data by employees, by ticking one of five available choices. The results revealed that more than one-third of respondents (34.6 percent) believed that accidental entry of bad data by employees happened between once a year and monthly; Almost 20 percent of the respondents believed this might happen from once a month to weekly; 18.4 percent of the respondents believed that accidental entry of incorrect data by employees very rarely happened in their banks, since it occurred less than once a year; while 1.5 percent of the respondents confirmed that never ever happened in their organizations.

On the other hand, 22.1 percent of the respondents claimed the frequent occurrence of accidental entry of incorrect data, between once a week to daily; while 7.3 percent of them believed that it happened daily or more frequently in their organizations. Many respondents qualified their report, stating that no harm is done as long as such mistakes are discovered and corrected in the final or half-day audit reports. The statistical results of both the Kruskal-Wallis test (Appendix 2) and the one-way ANOVA test (Appendix 3) show no significant differences among different Saudi organizations regarding the frequency of occurrence of accidental entry of bad data by employees (at $p = 0.05$). According to the statistical results, the following hypothesis: "There is no significant difference between different Saudi organizations regarding the accidental entry of bad data by their employees" could be accepted at significance level $p = 0.05$.

Intentional Entry of Bad Data by Employees

To investigate the respondents' opinions regarding the occurrence of intentional entry of bad data by employees, the respondents were asked to indicate the frequency of this threat. The statistics show that merely half of respondents (49.4 percent) expressed belief that it happened very rarely in their organizations, being likely to occur even less than once a year. Almost 23 percent of the respondents believed that intentional entry of incorrect data rarely occurred in their organizations, happening once a year to monthly; while 10 percent of the respondents believed that never happen before in their organizations. They considered it as a crime and a kind of computer fraud; therefore, whoever committed such a crime should be prosecuted.

On the other hand sex respondents (4.4 percent) believed that intentional entry of incorrect data by employees happened relatively frequently in their organizations, happening once a week to daily; while four respondents (2.9 percent) believed that might happen daily or more frequently due to the large, scattered number of the transactions and, moreover, the inadequacy of implemented controls. They too, considered that legal action should be taken against whoever commits it. The result of the Kruskal-Wallis (Appendix 2) and the one-way ANOVA (Appendix 3) tests provide evidence that there are no significant differences between the different organizations ($p = 0.05$). According to the obtained statistical results, the following hypothesis could be accepted at significance level $p = 0.05$: "There is no significant difference between different Saudi organizations regarding the intentional entry of bad data by their employees".

Accidental Destruction of Data by Employees

To understand the respondents' opinions regarding unintentional destruction of data by employees, the respondents were asked to indicate the frequency of its occurrence as a result of error or mistake. It is observed that 37.5 percent of the respondents believed that the frequency of accidental destruction of banks' data as a result of employees' errors or mistakes was less than once a year; while 9.6 of the respondents claimed that never happened before in their organizations. 29.4 percent of the respondents indicated that that could happen once a year to monthly and 18.4 percent of respondents believed that accidental destruction of data might happen once a month to weekly. On the other hand 4.4 percent of the respondents believed that accidental destruction of data by employees happened relatively frequently in their organizations, happening once a week to daily; while one respondent believed that might happen daily or more frequently.

When the respondents were interviewed, some of them mentioned that it would not be surprising if such destruction occurred, bearing in mind that their organizations have several departments and that a lot of new employees are hired every year who need more training. It was seen as an inconsequential threat, since data could be easily recovered through the organization excellent back up system. According to the results of the Kruskal-Wallis (Appendix 2) and one-way ANOVA tests (Appendix 3) it appears that there is no significant difference between the different Saudi organizations regarding the frequency of accidental destruction of data (at $p = 0.05$). Accordingly, the following hypothesis could be accepted at significance level $p = 0.05$: "There is no significant difference between different Saudi organizations regarding the accidental destruction of data by their employees".

Intentional Destruction of Data by Employees

Respondents were then asked to indicate their opinions regarding the occurrence of intentional destruction of data by employees. The statistical findings revealed that almost 60 percent of the respondents believed that this very rarely occurred in their organizations, since it might happen less than once a year; 12.5 of the respondents believed it had never ever happened; while 16.2 percent of the respondents believed that might happen once a year to monthly. However, a minority of the respondents (8.8 percent) mentioned that it could occasionally, but not frequently, happen, and only one respondent expressed his opinion that might happened daily triggered by some slight embezzlement by employees. Thus, it is observed that the frequency of intentional destruction seems to be quite low in the Saudi organizations.

However, both Kruskal-Wallis (Appendix 2) and one-way ANOVA tests (Appendix 3) provide strong evidence that there is no significant difference among the different Saudi organizations regarding the frequency of intentional destruction of data by their employees (at $p = 0.05$). According to the obtained statistical results, the following hypothesis could be accepted at significance level $p = 0.05$: "There is no significant difference between different Saudi organizations regarding the intentional destruction of data by their employees".

Unauthorized Access to the Data and / or System by Employees

To explore the frequency of unauthorized access to the banks' data / accounting systems by their employees, the respondents were asked to indicate the frequency of occurrence of such action in their organizations by ticking one among five available choices. . It is observed that

slightly more than two-third of the respondents (67.6 percent) claimed that unauthorized access to their CAIS rarely happened. They reported that it might occur less than once a year, due to secure implemented password systems; while 11 percent of respondents believed that had never happened. A minority of respondents (10.3 percent) believed that unauthorized access to their organizations' accounting systems by internal employees might occur once a year to monthly; 9.6 of the respondents believed that might occur once a month to weekly; and only 1.5 percent of respondents believe that it might happen once a week to daily, which can still be considered as a very low level of occurrence. According to the above result, unauthorized access to accounting systems / data by employee seems to be an infrequent security threat in the Saudi organizations.

The Kruskal-Wallis (Appendix 2) and one-way ANOVA tests (Appendix 3) provide strong support that there are no significant differences among different Saudi organizations regarding the frequency of unauthorized access to the accounting systems / data by their employees (p =. 05). According to the above results, the following hypothesis: "There is no significant difference between different Saudi organizations regarding the frequency of unauthorized access to the accounting systems / data by their employees" could be accepted at significance level p = 0.05.

Unauthorized Access to the Data and / or System by Outsiders

To investigate the existence and the frequency of unauthorized access to the data and/or systems by outsiders (hackers) in the Saudi organizations, the respondents were asked to indicate the frequency of that security threat in their organizations. The statistical results revealed that, the vast majority of the respondents (69.1 percent) indicated that it rarely happened in their organizations: less than once a year; and 12.5 percent of the respondents claimed that that never happened in their organizations. However, 10.3 percent of the respondents believed that it could happen once a year to monthly.

One possible interpretation of this result is that electronic services (such as E-business; phone banking; electronic fund transfer and corporate-banking) are not widespread and accepted in the Saudi organizations. On the other hand, four respondents, representing 2.9 percent of responses believed that unauthorized access to the data and / or systems by outsiders (hackers) happened once a month to weekly, again another four respondents indicated that it occurred once a week to daily, while another three respondents (representing 2.2 percent) affirmed that it happened more frequently in their organizations. The Kruskal-Wallis test (Appendix 2) and the one-way AVOVA (Appendix 3) tests show no indicate significant differences among different Saudi organizations (at significance level p = 0.05). Thus, the following hypothesis "There is no significant difference among the different Saudi organizations regarding the frequency of Unauthorized access to their data / systems by outsiders" would be accepted.

Employees' Sharing of Passwords

To explore the frequency of employees' sharing of passwords in the Saudi environment, the respondents were asked to indicate its occurrence in their organizations. The result shows that almost 10 percent of the respondents believed that sharing of passwords seldom occurred in their organizations. However, 44.1 percent of respondents reported that it very rarely occurred: less than once a year to monthly; and 19.1 percent of respondents believed that it rarely happened: from once a year to monthly. On the other hand almost 9 percent of

respondents reported that sharing passwords happened once a month to weekly; 9.6 of respondents believed it happened once a week to daily; while 8.8 of respondents believed that sharing password is more frequent in their organizations: happening daily or more frequently. It is also observed that 27.2 percent of the respondents believed that sharing of passwords occurred more than once a year to monthly; the results tend to suggest the high level of occurrence of employees' sharing of passwords in the Saudi organizations.

The statistical results of both the Kruskal-Wallis test (Appendix 2) and the one-way ANOVA test (Appendix 3) show no significant differences among different organizations regarding the frequency of employees' sharing of passwords in the Saudi environment (at significance level $p = 0.05$). According to the above statistical results, the following hypothesis could be accepted (at significance level $p = 0.05$): "There is no significant difference among different Saudi organizations regarding the frequency of occurrence of employees' sharing of passwords".

Natural Disasters

In relation to the frequency of occurrence of natural disaster in the Saudi organizations, respondents were asked to indicate its occurrence in their organizations. According to Parker (1976) "Natural disasters caused by fire, water, wind, power outages, lightning, and earthquakes could cause significant disruption (or even destruction) of computer facilities, or at least crucial parts of computer facilities" (p. 14). The results showed that the majority of respondents (approximately 71.3 percent) confirm the rarity of natural disasters in the Saudi organizations; while 10.3 percent believed that never happened in their organizations. Such natural disaster as earthquakes or loss of electricity occasionally happened, but less than once every several years. Moreover, water floods and wind disasters very rarely occur in Saudi Arabia. 12.5 percent of the respondents believed that it could happen once a year to monthly, while only less 6 percent of respondents believed that natural disaster (such as loss of power supply) might occur once a month to weekly or more.

The statistical result of both Kruskal-Wallis (Appendix 2) and one-way ANOVA tests (Appendix 3) show no significant differences among the different Saudi organizations regarding the reported threat from frequency of occurrence of natural disasters (at $p = 0.05$). Relying on the above results, the following hypothesis could be accepted (at significance level $p = 0.05$): "There is no significant difference among different Saudi organizations regarding the frequency of occurrence of natural disasters".

Disasters of Human Origin

Man-made disasters include those disasters caused by people, such as fires, floods and explosions. However, man-made disasters could occur as a result of intentional or accidental human actions. Many intentional acts are classified as crimes, such as fraud, theft, embezzlement, extortion, larceny and mischief. To investigate the frequency of such man-made disaster in the Saudi organizations, the respondents were asked to indicate its occurrence in their banks. The statistical results revealed that 70.3 of respondents considered that man-made disaster is a very rare event in their organizations, with an occurrence of less than once a year; while 10 percent of respondents confirmed that such man-made disaster had never happened before. Another 12.3 percent of respondents reported that this threat was rarely encountered in their organizations.

Only 8 respondents (5.9 percent) believed that it happened once a month to weekly ore more. The above results provide an indicator on the low reported frequency of man-made disasters in the Saudi organizations. The statistics from both Kruskal-Wallis (Appendix 2) and one-way ANOVA tests (Appendix 3) provide strong evidence that there are no significant differences among the different bank types regarding the frequency of man-made disaster in the Saudi organizations (at significance level $p = 0.05$). This suggests that the hypothesis that "There is no significant difference among the different Saudi organizations regarding the frequency of man- made disasters" should be accepted (at significance level $p = 0.05$).

Introduction (Entry) of Computer Viruses to the Systems

To investigate the threat from the introduction of computer viruses to the Saudi organizations' accounting systems, respondents were asked to indicate the occurrence of this threat in their organizations. Slightly more than half of the respondents (52.2 percent) reported that the introduction of computer viruses seldom occurred: its probability was less than once a year; and 9.5 of respondents confirmed that that had never happened in their organizations. Again, 22.1 percent of the respondents believed that it happens once a year to monthly; while 8.8 percent of respondents believed it occurred once a month to weekly. Only five respondents (2.2 percent) believed that the introduction of computer viruses happened once a week to daily and 3 respondents (2.2 percent) reported that the introduction of computer viruses was more frequent in their organizations: happing daily or more frequently. Based on the finding above, it is observed that the reported frequency of introduction of computer viruses could be considered quite high in the Saudi organizations. The possible reason behind this could be that some of Saudi organizations were not booting the original programs and software packages.

According to the result of the Kruskal-Wallis (Appendix 2) and one-way ANOVA tests (Appendix 3) it seems that there are no significant differences among the different Saudi organizations groups regarding the frequency of the introduction of computer viruses (at significance level $p = 0.05$). Relying on the above statistical results the following hypothesis could be accepted (at significance level $p = 0.05$): "There is no significant difference among the different Saudi organizations regarding the frequency of introduction of computer viruses to their banks' CAIS".

Suppression or Destruction of Output

In order to explore the frequency of suppression or destruction of output in the Saudi organizations, the respondents were asked to indicate its frequency in their organizations. The statistics show that the majority of respondents (59.6 percent) believed that suppression or destruction of their organizations' output occurred less than once a year; while 11 percent of the respondents confirmed suppression or destruction of output never happened in their organizations. A further 14 percent of the respondents confirmed the occurrence of that security threat to be rare. On the other hand 21 respondents, representing 15.5 percent of the total, believed that suppression or destruction of their organizations' output occurred more than once a week to monthly. The above finding provides great support for the low frequency of the suppression or destruction of CAIS' output in the Saudi organizations.

The statistical results of both Kruskal-Wallis (Appendix 2) and one-way ANOVA tests (Appendix 3) provide empirical evidence that there are no significant differences among the different Saudi organizations regarding the frequency of the suppression or destruction of

their CAIS' output in the Saudi organizations (at p = 0.05). Accordingly, the hypothesis "There is no significant difference among the different Saudi organizations regarding the frequency of suppression or destruction of CAIS' output" could be accepted (at significant level p = 0.05).

Creation of Fictitious / Incorrect Output

To explore the frequency of creation of fictitious / incorrect output in the Saudi organizations, the respondents were asked to indicate the frequency of occurrence of that security threat in their organizations by ticking the appropriate frequency of the threat among five available choices. The findings reveal that slightly more half of the respondents (55.1 percent) believed that creation of fictitious / incorrect output rarely happened: occurring less than once a year; while 9.6 of the respondents believed that creation of fictitious / incorrect output is never happened in their organizations. A minority of respondents (21.3 percent) believed that creation of fictitious / incorrect output might occur once a year to monthly, which can still be considered as a low level of occurrence. On the other hand, only 15 percent of the respondents reported that creation of fictitious / incorrect output occurred more than once a year to monthly. According to the above result, the creation of fictitious / incorrect output seems to be a low-level security threat in the Saudi organizations. The statistical results of the Kruskal-Wallis (Appendix 2) and one-way ANOVA tests (Appendix 3) provide evidence that there are no significant differences among different Saudi organizations regarding the frequency of creating fictitious / incorrect CAIS' output (p = 0.05). Therefore, the hypothesis that: **"**There is no significant difference among Saudi organizations regarding the frequency of creating fictitious / incorrect CAIS' output" could be accepted (at significance level p = 0.05).

Theft of Data / Information

Respondents were asked to indicate the frequency of data theft in their organizations. The great majority of the respondents (approximately 70 percent) indicated that theft of data / information was rare in their organizations, since it might occur less than once a year; and 9.6 of the respondents reported that theft of data / information never happened in their organizations. However, 13.2 percent of the respondents believed that it could happen once a year to monthly and the minority of the respondents (less than 9 percent) believed that theft of data / information happened more than once a year to monthly. The results suggested that theft of data / information have a low level occurrence in the Saudi organizations. The result of both the Kruskal-Wallis (Appendix 2) and one-way ANOVA tests (Appendix 3) suggest these differences are not significant, however (at p = 0.05). Relying on the above statistical results, the hypothesis: "There is no significant difference among different organizations regarding the frequency of theft of data / information in the Saudi environment" could be accepted (at p = 0.05).

Unauthorized Copying of Output

To investigate the frequency of Unauthorized copying of output in the Saudi organizations, the respondents were asked to indicate its occurrence in their organizations. The results revealed that vast majority of the respondents (66.9 percent) reported that Unauthorized copying of output was rare, since it occurred less than once a year; and 11 percent of the respondents claimed that that never happened in their organizations. However, a minority (13.2 percent) believed that it occurred once a year to monthly. On the other hand, four

respondents, representing 2.9 percent of responses believed that Unauthorized copying of output happened once a month to weekly, again a similar percentage of the respondents indicated that it occurred once a week to daily. Again, another four respondents (representing 2.9 percent) affirmed that it happened more frequently in their organizations.

The result provides an indicator of the low frequency of unauthorized copying of output in the Saudi organizations. The statistical result of both Kruskal-Wallis (Appendix 2) and one-way ANOVA tests (Appendix 3) provide strong evidence that the differences are non-significant among the different organization types (at significance level $p = 0.05$). Based on the above statistical results, the following hypothesis could be accepted (at significance level $p = 0.05$): "There is no significant difference among the different types of organizations regarding the frequency of unauthorized copying of CAIS' output in the Saudi environment".

Unauthorized Document Visibility

Respondents were asked to indicate the frequency of this threat in their organizations by ticking one of five available choices. The statistics revealed that approximately 60 percent of the respondents believed that unauthorized document visibility, by displaying it on monitors or printed on paper, was very rare, as it occurred less than once a year, while 6.6 of the respondents believed that it is never happened in their organizations. However, 16.2 of the respondents reported that unauthorized document visibility happened once a year to monthly; and 8.8 percent believed that it occurred once a month to weekly. On the other hand 6 percent of the respondents believed that unauthorized document visibility occurred once a week to daily and only 3.7 percent of the respondents believed that might happened daily or more frequently which still considered as a very low level of occurrence.

According to the above result, unauthorized document visibility seems to be a very low level threat in the Saudi organizations. The Kruskal-Wallis (Appendix 2) and one-way ANOVA tests (Appendix 3) provide no evidence of significant difference among different organizations' types regarding the frequency of unauthorized document visibility (at $p = 0.05$). Relying on the previous results the following hypothesis could be accepted: "There is no significant difference among different organizations' types regarding the frequency of unauthorized document visibility in the Saudi organizations".

Unauthorized Printing and Distribution of Data / Information

In order to explore the frequency of unauthorized printing and distribution of information in the Saudi organizations, the respondents were asked to indicate its occurrence in their organizations. The result shows that the majority of respondents (60.3 percent) considered the frequency of unauthorized printing and distribution of information to be extremely low (less than once a year) and 10.3 percent of the respondents reported that unauthorized printing and distribution of information never happened in their organizations; while approximately 17 percent of respondents believed that it happened between once a year to monthly in their organizations. On the other hand, 5.9 percent of the respondents believed that unauthorized printing and distribution of information happened between once a month to weekly, less than 3 percent of the respondents reported that it might occur once a week to daily; and only 3.7 of the respondents believed unauthorized printing and distribution of information occurred daily or more frequently in their organizations. The results provide evidence of the low frequency of unauthorized printing and distribution of information in the Saudi organizations.

The statistical results of both Kruskal-Wallis (Appendix 2) and one-way ANOVA tests (Appendix 3) show no significant differences among the different Saudi organizations types regarding the frequency of unauthorized printing and distribution of information (at significance level p = 0.05). According to the obtained statistical results, the following hypothesis could be accepted (at significance level p = 0.05) **"**There is no significant difference among the different organizations types regarding the frequency of unauthorized printing and distribution of information in the Saudi environment".

Directing Prints And Distributed Information To People Not Entitled To Receive

To investigate the existence and the frequency of misdirection of prints and distributed information to individuals not entitled to receive them, the respondents were asked to indicate the frequency of that security threat in their organizations. The statistics revealed that 55.1 percent of respondents indicated that this threat was very rarely encountered in their organizations (less than once a year) while 8.1 of the respondents believed that never happened in their organizations before. However, 22.1 percent of the respondents believed that it happened once a year to monthly. On the other hand, 8.1 percent of the respondents mentioned that it occurred once a month to weekly; only one respondent believed that occurred once a week to daily and eight respondents (representing 5.6 percent) believed that misdirection of prints and distributed information to individuals not entitled to receive them were more frequent in their organizations: happened daily or more frequently.

Both Kruskal-Wallis (Appendix 2) and one-way ANOVA tests (Appendix 3) show no significant differences between the different organizations' types regarding the frequency of misdirection of prints and distributed information (at p = 0.05). In the light of the above statistical results, the following hypothesis could be accepted (at p = 0.05): "There is no significant difference among the different Saudi organizations regarding the frequency of directing prints and distributed information to individuals who are not entitled to receive them"

Sensitive Documents are handed to Non- Security Cleared Personnel for Shredding

To investigate the threat from handling sensitive documents, respondents were asked to indicate the occurrence of this security threat in their organizations. The majority of respondents (61 percent) reported that handing sensitive documents to non-security-cleared personnel for shredding very rarely occurred; 8.8 of the respondents claimed that it had never happened before; and 19 percent of the respondents reported that handling sensitive documents to non-security cleared individuals for shredding happened once a year to monthly in their organizations. A minority of respondents (11 percent) believed that this might happen more than once a year to monthly. These findings strongly support the view that the frequency of handing sensitive documents to non-security cleared personnel for shredding is quite low in the Saudi organizations. The statistics from both the Kruskal-Wallis test (Appendix 2) and the one-way ANOVA test (Appendix 3) show non-significance of differences among the different Saudi organizations regarding this threat (at p = 0.05). Based on the above findings the following hypothesis could be accepted (at significance level p = 0.05): "There is no significant difference among different Saudi organizations regarding the frequency of handling sensitive documents to non-security cleared personnel for shredding"

Interception of Data Transmissions

In an attempt to explore the frequency of interception of data transmissions from remote locations in the Saudi organizations, the respondents were asked to indicate its occurrence in their organizations. Again, it is observed that approximately 60 percent of respondents considered that the frequency of interception of data transmission very rarely occurred in their organization; and 11 percent of the respondents claimed that never happened before. However, 17.6 percent of respondents reported that it occurred once a year to monthly; 5.9 of respondents reported that it happened once a month to weekly, only two respondents (1.5 percent) believed that interception of data transmissions occurred once a month to weekly; and only 4.4 percent of the respondents believed that interception of data transmissions from remote locations is more frequent in their organizations. The above results suggest that the frequency of this threat is quite low in the Saudi environment.

The statistical result of both Kruskal-Wallis (Appendix 2) and one-way ANOVA (Appendix 3) tests show no significant differences among the different Saudi organizations regarding this threat (at $p = 0.05$). Relying on the above results, the following hypothesis could be accepted (at significance level $p = 0.05$): "There is no significant difference among different organizations regarding the frequency of data transmissions from remote locations in the Saudi environment"

CONCLUSION AND RECOMMENDATIONS FOR FURTHER RESEARCH

The main objective of this paper was to investigate the significant perceived security threats of CAIS, through their frequency of occurrence, in the Saudi organizations. A list of CAIS security threats was developed based on the previous studies (for example, Loch et al., 1992; Davis, 1996 and Henry, 1997, and Abu-Musa 2001) and available literature in this area. However, some other security threats were suggested and included in this list to be investigated for the first time in the Saudi environment. The results reported that accidental and intentional entry of bad data by employees, accidental destruction of data by employees, introduction of computer viruses to the system, employees' sharing of passwords; suppression and destruction of output; unauthorized document visibility; and misdirecting prints and distributing information to people not entitled to receive them are the most perceived significant security threats to CAIS in the Saudi organizations.

The results of Kruskal-Wallis and ANOVA tests show that there are no significant differences between different organizations' types regarding the frequency of occurrence of CAIS security threats in the Saudi environment. However, further research could be undertaken to extend and improve this research. The current research intended to investigate the security threats of CAIS in the Saudi organizations. More research is needed to have evidence from other developing countries. A comparative study could be carried out to investigate the significant differences between developing and developed countries regarding the CAIS security issues investigated.

REFERENCES

Abu-Musa, Ahmad A. (2001), Evaluating The Security of Computerized Accounting Information Systems: An Empirical Study on Egyptian Banking Industry", ***PhD. Thesis***, Aberdeen University, UK.

Abu-Musa, Ahmad A. (2003), "The Perceived Threats to the Security of Computerized Accounting Information Systems", ***The Journal of American Academy of Business, Cambridge, USA***, Vol. 3, No.1, September, pp. 9- 20.

Collier, Paul, Rob Dixon and Claire Marston (1991), "The Role of Internal Auditor in the Prevention and Detection of Computer Fraud", ***Public Money and Management,*** (Winter), pp. 53 - 61.

Dougan, Jim (1994), "Internal Control Checklist for Hospitality Computer Systems", ***Bottom Line,*** (Vol. 9, Iss. 5), pp. 8 - 11.

Davis, Charles E. (1996), "Perceived Security Threats to Today's Accounting Information Systems: A Survey of CISAs", ***IS Audit & Control Journal,*** (Vol. 3), pp. 38 - 41.

Davis, Charles E. (1997), "An Assessment of Accounting Information Security", ***The CPA Journal,*** New York (Vol. 67, Iss. 3), pp. 28 - 34.

FFIEC (1996) ***IS Examination Handbook, Chapter, 14, Security- Physical And Data.***

Grundy, Emma, Collier, Paul and Spaul, Barry (1994), "Auditing Personnel: A Human Resource Approach to Information System Control", ***Managerial Auditing Journal,*** (Vol. 9), pp. 10-16.

Haugen Susan and J. Roger Selin (1999), "Identifying and Controlling Computer Crime and Employee Fraud", ***Industrial Management and Data Systems,*** (Vol. 99, Iss. 8).

Henry, Laurie (1997), "A Study of the Nature and Security of Accounting Information Systems: The Case of Hampton Roads, Virginia", ***The Mid-Atlantic Journal of Business,*** (Vol. 33, Iss. 63), pp. 171 - 189.

Hood, Keith L. and Jie-Win Yang (1998), "Impact of Banking Information Systems Security on Banking in China: The Case of Large State-Owned Banks in Shenzhen Economic Special Zone - An Introduction", ***Journal of Global Information Management,*** (Vol. 6, No. 3), pp. 5 - 15.

Jenkins, Brian, Peter Cooke and Peter, Quest (1992), ***An Audit Approach to Computers,*** Institute of Chartered Accountants In England And Wales, London.

Leinicke, Linda Marie, W. Max Rexroad and Jon D. Ward (1990), "Computer Fraud Auditing: It Works", ***Internal Auditor,*** (Vol. 47 Iss. 4), pp. 26 - 33.

Levi, Philip (1993), "PC security for accountants - What's Hot and What's New", ***Accounting Technology,*** (Feb. / Mar.), pp. 26-30.

Loch, Karen D., Houston H. Carr and Merrill E. Warkentin (1992), "Threats to Information Systems: Today's Reality, Yesterday's Understanding", ***MIS Quarterly,*** (June), pp. 173 - 186.

National Institute of Standards and Technology (1995), Technology Administration, U.S. Department of Commerce, ***An Introduction to Computer Security: The NIST Handbook***, Special Publication 800-12. October 1995

Parker, Donn B. (1976), ***Crime By Computer,*** Charles Scribner's sons, New York.

Roufaiel, Nazik S. (1990), "Computer Related Crimes: An Educational And Professional Challenge", ***Managerial Auditing Journal,*** (Vol. 5, Iss. 4), pp. 18 - 25.

Ryan, S. D. and B. Bordoloi (1997), "Evaluating Security Threats in Mainframe and Client / Server Environments", ***Information & Management,*** (Vol. 32, Iss. 3), pp. 137 - 142.

Schweitzer, James A. (1987), ***Computers, Business, and Security,*** Butterworth Publishers, London.

(Appendix: 1)
(The Questionnaire Used In the Empirical Survey)

King Fahd University of Petroleum & Minerals
College of Industrial Management
Department of Accounting & Management Information Systems

INVESTIGATING THE PERCEIVED THREATS OF COMPUTERIZED ACCOUNTING INFORMATION SYSTEMS IN DEVELOPING COUNTRIES: AN EMPIRICAL STUDY ON SAUDI ORGANIZATIONS

Dear Sir/

My research topic is "Investigating the Perceived Threats of Computerized Accounting Information Systems in Developing Countries: An Empirical Study on Saudi Organizations". The research objective is to investigate the significant perceived threats of computerised accounting information systems in Saudi companies. I would be very grateful if you would complete the enclosed questionnaire. We want to confirm that the information gathered from this survey will be confidential and its use is only for academic research purposes. Your participation and your answers are very important to this research, and we would ask you to respond correctly and carefully. Your participation and prompt response is much appreciated.

Thank you very much for your help and considerations

Yours Sincerely,

Dr. Ahmad Abu-Musa

Dr. Ahmad A. Abu-Musa
Department of Accounting and MIS
College of Industrial Management
King Fahd University of Petroleum and Minerals
P O Box 1755, Dhahran, 31261, Saudi Arabia
Phone: 00966-3-860-1420
Fax: 00966-3-860-3489
mailto:abumusa@kfupm.edu.sa

1. Your Accounting Information System

The main objective of this section is to collect some information regarding the nature your computerized accounting information systems.

1. Do you currently work in?

❒ Manufacturing
❒ Banking
❒ Insurance
❒ Health Care
❒ Retail Merchandising
❒ Wholesale Merchandising
❒ Government
❒ Other - please list _____

2. How many accounting professionals are employed in your firm?

❒ 1- 50 ❒ 51-100
❒ 101-150 ❒ 151-200
❒ Over 200

3. How many information system specialists are employed in your firm?

❒ 1- 5 ❒ 6-10
❒ 11-15 ❒ 16-20
❒ Over 20

4. What is your current job title?

❒ Internal auditor
❒ Staff accountant
❒ Cost accountant
❒ Controller
❒ EDP auditor
❒ Other - please list _____

5. How many years of experience do you have at your current position? _____

6. Your accounting system is: (Please, tick)

❒ Manual, no computers are used.
❒ A combination of manual and computer processed.
❒ Strongly computerized.

2. Assessment of the Threats of Accounting Information Systems

The main objective of this section is to investigate the main threats that actually face the computerized accounting system security in the Saudi banks, and the relative materiality of each threat.

Please, indicate the frequencies of each threat by ticking the appropriate place:

Accounting information systems threats	*Less than Once a year*	*Once a year to monthly*	*Once a month to weekly*	*Once a week to daily*	Daily or more frequen tly
1. Accidental entry of bad data by employees is					
2. Intentional entry of bad data by employees is					
3. Accidental destruction of data by employees is					
4.Intentional destruction of data by employees is					
5. Unauthorized access to the data and / or system by employees is					
6. Unauthorized access to the data and / or system by outsiders (hackers) is					
7. Employees' sharing of passwords is					
8. Natural disaster such as fire, flooding, loss of power, is					
9. Human- made disasters such as fire, loss of power, is					
10. Introduction (entry) of computer viruses to the system is					
11. Suppression or destruction of output is					
12. Creation of fictitious / incorrect output is					
13. Theft of data / information is					
14. Unauthorized copying of output is					
15. Unauthorized document visibility by displaying on monitors or printed on paper is					
16. Printing and distribution of information by unauthorized persons.					
17. Prints and distributed information are directed to people who are not entitled to receive it.					
18. Sensitive documents are handed to non- security cleared personnel for shredding.					
19. Interception of data transmissions from remote locations is					

Appendix: 2

(Kruskal-Wallis Test)

Test Statistics[a,b]

	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	Unauthorised access to the data and / or system by employees	Unauthorised access to the data and / or system by outsiders	Employees' sharing of passwords
Chi-Square	8.009	10.748	15.009	15.290	8.474	5.771	2.649
df	8	8	8	8	8	8	8
Asymp. Sig.	.433	.216	.059	.054	.389	.673	.954

a. Kruskal Wallis Test

b. Grouping Variable: The Type of Business

Test Statistics[a,b]

	Natural disaster	Human-made disasters	Introduction (entry) of computer viruses to the system	Suppression or destruction of output	Creation of fictitious / incorrect output	Theft of data / information
Chi-Square	8.367	5.677	8.169	7.569	12.381	10.723
df	8	8	8	8	8	8
Asymp. Sig.	.398	.683	.417	.477	.135	.218

a. Kruskal Wallis Test

b. Grouping Variable: The Type of Business

Test Statistics[a,b]

	Unauthorised copying of output	Unauthorised document visibility	Unauthorised printing and distribution of information	Prints and distributed information are directed to people who are not entitled to receive it.	Sensitive documents are handed to non- security cleared personnel for shredding.	Interception of data transmissions from remote locations
Chi-Square	6.998	4.886	5.383	8.280	7.769	7.342
df	8	8	8	8	8	8
Asymp. Sig.	.537	.770	.716	.407	.456	.500

a. Kruskal Wallis Test

b. Grouping Variable: The Type of Business

Appendix: 3

(Kruskal -Wallis Test)

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Accidental entry of bad data by employees	Between Groups	11.648	8	1.456	1.004	.437
	Within Groups	184.227	127	1.451		
	Total	195.875	135			
Intentional entry of bad data by employees	Between Groups	20.912	8	2.614	.980	.455
	Within Groups	338.728	127	2.667		
	Total	359.640	135			
Accidental destruction data by employees	Between Groups	25.803	8	3.225	1.469	.175
	Within Groups	278.837	127	2.196		
	Total	304.640	135			
Intentional destruction data by employees	Between Groups	21.850	8	2.731	.954	.475
	Within Groups	363.679	127	2.864		
	Total	385.529	135			
Unauthorised access to the data and / or syster by employees	Between Groups	19.713	8	2.464	.944	.483
	Within Groups	331.633	127	2.611		
	Total	351.346	135			
Unauthorised access to the data and / or syster by outsiders	Between Groups	13.213	8	1.652	.525	.836
	Within Groups	399.603	127	3.146		
	Total	412.816	135			
Employees' sharing of passwords	Between Groups	8.490	8	1.061	.337	.950
	Within Groups	399.481	127	3.146		
	Total	407.971	135			
Natural disaster	Between Groups	18.093	8	2.262	.837	.571
	Within Groups	343.017	127	2.701		
	Total	361.110	135			
Human- made disaster	Between Groups	10.271	8	1.284	.470	.875
	Within Groups	346.839	127	2.731		
	Total	357.110	135			

Appendix: 3

(ANOVA Test)

ANOVA

		Sum of Squares	df	Mean Square	F	Sig.
Introduction (entry) of computer viruses to th system	Between Group	15.164	8	1.895	.732	.663
	Within Groups	328.954	127	2.590		
	Total	344.118	135			
Suppression or destruction of output	Between Group	11.827	8	1.478	.497	.857
	Within Groups	377.931	127	2.976		
	Total	389.757	135			
Creation of fictitious / incorrect output	Between Group	18.117	8	2.265	.897	.521
	Within Groups	320.522	127	2.524		
	Total	338.640	135			
Theft of data / informa	Between Group	21.595	8	2.699	1.009	.433
	Within Groups	339.750	127	2.675		
	Total	361.346	135			
Unauthorised copying output	Between Group	9.154	8	1.144	.385	.927
	Within Groups	377.486	127	2.972		
	Total	386.640	135			
Unauthorised docume visibility	Between Group	9.844	8	1.231	.516	.843
	Within Groups	303.148	127	2.387		
	Total	312.993	135			
Unauthorised printing and distribution of information	Between Group	6.088	8	.761	.262	.977
	Within Groups	368.728	127	2.903		
	Total	374.816	135			
Prints and distributed information are directe to people who are not entitled to receive it	Between Group	12.072	8	1.509	.588	.786
	Within Groups	325.663	127	2.564		
	Total	337.735	135			
Sensitive documents a handed to non- securit cleared personnel for shredding	Between Group	13.427	8	1.678	.659	.726
	Within Groups	323.213	127	2.545		
	Total	336.640	135			
Interception of data transmissions from remote locations	Between Group	18.087	8	2.261	.771	.629
	Within Groups	372.317	127	2.932		
	Total	390.404	135			