. *King Saud Univ.,* Vol. 18, *Comp. & Info. Sci*., pp. 1-26 (A.H. 1426/2006)

Investigating the Perceived Threats of Computerized Accounting Information Systems in Developing Countries: An Empirical Study on Saudi Organizations

Ahmad A. Abu-Musa*
Department of Accounting & MIS, KFUPM, Saudi Arabia

(Received 22 May 2004; accepted for publication 20 February 2005)

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

1. Introduction

The rapid change in information technology, the wide spread of user-friendly systems and the great desire of organizations to acquire and implement up-to-date computerized systems and software have made computers much easier to be used and enabled accounting tasks to be accomplished much faster and accurate than hitherto.

* Dr Ahmad A. Abu-Musa is an 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.

On the other hand, this advanced technology has also created significant risks related to ensuring the security and integrity of computerized accounting information systems (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 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.

2. Literature Review

Reviewing the literature concerned with evaluating the security of computerized 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 computerized information systems in an organization; to explore the significance of such perceived security threats in the real world; and to investigate their occurrence and potential losses in different organizations.

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 Executives regarding the security threats in microcomputer, mainframe computer, and network environments. The researchers developed a list of twelve security threats and empirically examined. The results indicated that natural disasters; employee accidental actions (entry of bad data and destruction of data); inadequate control over media; and unauthorized access to CAIS by hackers had been ranked among the top security threats. These results confirmed the experts' claims that the greatest threats come from inside organizations.

Since accounting information system security has become one of the major concerns for information system auditor, Davis (1996) tried to discover the current status of the security issue in practice. Davis conducted a survey using 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 information systems auditors recognized that different computing environments have different relative levels of security risks.

The results of Davis' (1996) study also reported that 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.

Ryan and Bordoloi (1997) explored how companies moving from a mainframe to a client/server environment evaluated and took security measures to protect against potential security threats. The results of Ryan and Bordoloi's (1997) study revealed that the most 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; and single point of failure.

Henry (1997) conducted a survey to determine the nature of the accounting systems and security in use. 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 utilized protection from viruses. Physical security and authorization 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 utilizing some form of communication hardware. Almost 45 percent of the sample underwent some sort of audit of CAIS data.

In 1998, Hood and Yang studied the impact of banking information systems security on banking in China in comparison to the UK. The survey results revealed that all respondents believe that management was aware of security but none believed that their banks had taken enough action to reduce the risks and losses. The most common reason for this was the lack of financial and human resources. Furthermore, all four banks surveyed claimed to have a security policy, but only in one was formally stated. Human security threats were perceived as the most important security threats in Chinese banking sector, especially malicious attack from outsiders.

Reviewing the nature of security breaches that occurred in different parts of the world, Dhillon (1999) argued that many of the security losses resulting form computer-related fraud could be avoided if organizations adopted a more pragmatic approach in dealing with such incidents as well as adopting a balanced approach of security controls which place equal emphasis on technical, formal and informal interventions to their computerized systems. The results of Dhillon's study (1999) suggested that implementing controls, as identified in a security policy, would indeed deter computer misuses. Committing computer fraud by insiders is recognized as a sever problem which could be difficult to prevent especially when it blends with legitimate transactions.

Siponen (2000) introduced a conceptual foundation for organizational information security awareness program to minimize the end-user errors and to enhance the effectiveness of implemented security controls. Siponen (2000) argued that information security techniques or procedures would lose their real usefulness if they were misused; misinterpreted; not used or not properly implemented by end-users.

Hermanson et al (2000) carried out an exploratory survey using a questionnaire to understand how organizations are addressing their IT risks and to examine evaluations of IT risks performed by internal auditors in their organizations. The results of the study revealed that internal auditors focus primarily on traditional IT risks and controls, such as IT asset safeguarding, application processing, and data integrity, privacy, and security.

Abu-Musa (2001) carried out a survey to investigate security threats of CAIS in the Egyptian banking sector (EBS). The entire population (Sixty-six banks' headquarters) of the EBS was surveyed using a self-administered questionnaire which

included nineteen CAIS security threats. The statistical results of the 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 EBS. The CAIS security threats list suggested by Abu-Musa (2001) will be adopted and used in the current study to investigate the significant perceived security threats challenging CAIS is Saudi environment.

Coffin and Patilis (2001) studied the role of internal auditors in evaluating the security controls of protecting sensitive data in CAIS in financial institutions such as Banks, securities firms, and insurance. The researchers argued that internal auditing could significantly help organizations in determining and evaluating the implemented security controls surrounding the collection, use and access to customer information as well as compliance with applicable regulations.

White and Pearson (2001) surveyed over two hundred USA companies to investigate the security controls of personal use of computers, controlling e-mail accounts, and securing company data. The results of the study reinforced the need for better security control in the majority of surveyed companies. The results also revealed that many corporations began to use computer technology before implementing appropriate safeguards; and the majority of the company's safeguards continue to be lacking.

Warren (2002) carried out a survey to investigate the security practices of computerized information systems in three countries: Australia; UK and USA. The paper attempted to evaluate security practices from different perspectives and to investigate whether the security practices are varied from one country to another. The results of survey revealed that:

- In Australia, poor levels of computer security were found among Australian organizations. Many of the security problems were identified due to poor security procedures being implemented. The results also indicated that 45 percent of organizations did not budget for computer security.
- In UK, 42 percent of organizations did not have an information security policy. The findings also revealed that 49 per cent of organizations listed budget constraints as being an issue in implementing computer security.
- While in USA, theft of information and financial fraud caused the most financial damage. However, differences in the levels of CAIS abuses carried out by internal and external individuals were not significant. The paper suggested that USA security practices seem to be more effective than those of Australia or the UK.

Wright and Wright (2002) conducted an exploratory study to obtain an understanding of unique risks associated with the implementation and operation of Enterprise Resource Planning (ERP) systems using a semi-structured interview approach. The research findings reported that the ERP system initially lacked adequate controls and that data conversion was also poorly executed. The potential for financial statement errors and business risks is further intensified as a result of the lack of proper user training. The findings also reported that ongoing risks differ across applications and across vendor packages. Finally, the results suggest that major firms use process audit techniques, as opposed to validation testing (i.e., they do not rely on tests of output) when hired to provide assurance on the risks for an ERP system.

Recently, The National Institute of Standards and Technology (2003) in USA issued its initial publication draft titled "Standards for Security Categorization of Federal Information and Information Systems". This publication establishes three potential levels of risk (low, moderate, and high) for each of the stated security objectives (confidentiality, integrity, and availability) relevant to securing computerized information systems. The proposed levels of risk are more heavily weighted toward the impact of risk on the security of CAIS and the potential magnitude of harm that the loss of confidentiality, integrity, or availability would have on agency operations (including mission, functions, image or reputation), agency assets, or individuals (data privacy).

The United States General Accounting Office (GAO) (2003) performed a review at the Financial Management Service (FMS) during the period from October 2002 to June 2003 to investigate whether FMS: (1) conducted a comprehensive security risk assessment and (2) documented and implemented appropriate security measures and controls for the system's protection. The results of GAO' review (2003) revealed that although FMS and the Federal Reserve had implemented numerous of security controls to protect their computing resources, risks were not sufficiently assessed, and numerous of security control weaknesses were identified. Accordingly immediate actions to correct the weaknesses to promptly address new security threats and risks as they emerge to CAIS were highly recommended.

In a very recent study, Hunton et al. (2005) carried out an experiment study to understand, assess and examine the extent to which financial auditors and information systems (IS) audit specialists recognize differences in the nature and unique business and audit risks associated with enterprise resource planning (ERP) systems, as compared to traditional computerized (non-ERP) systems. The research findings revealed that financial auditors were significantly less concerned than IS audit specialists with the following heightened risks of the ERP environment in the experimental case: business interruption, network security, database security, application security, process interdependency, and overall control risk. Moreover, financial auditors did not recognize the heightened risks of a seeded control weakness as well as reluctance to seek

consultation of IS audit specialists. However, IS audit specialists were less confident in financial auditors' abilities to recognize unique risks posed by ERP systems. The findings suggest a lack of understanding and consideration of unique ERP risks by financial auditors, which could have deleterious effects on audit quality.

3. The Importance of the Research

Reviewing the literature, it is observed that many of the previous studies (e.g., Loch et al. 1992; Davis, 1997; Ryan and Bordoloi, 1997; and Henry, 1997) did not always clearly distinguish between security threats and the inadequacy of security controls. The previous studies treated some inadequate or ineffective security controls as security threats. For examples, 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; poor segregation of information systems duties; poor segregation of accounting duties; inadequate control over storage media; inadequate audit trial, the inadequate or non-existence log-on procedures, loss due to inadequate backups or log files, uncontrolled read and / or update access, uncontrolled user privilege, and weak / ineffective or inadequate physical controls) were considered as security threats. This is confusion: weak policing does not itself create the crime. 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 organization. The researchers therefore included them in their survey and reported them as important to good information technology management and practice (p. 139).

In the current study, security threats and controls have been carefully distinguished. A selected number of precise security threats to CAIS are derived from previous studies (Loch et al., 1992; Davis, 1996 and 1997; FFIEC, 1996; and Henry, 1997). In addition, the following CAIS security threats are included in the proposed security list to be empirically examined for the first time is Saudi Arabia: human- made disasters such as fire, loss of power; suppression or destruction of output; creation of fictitious / incorrect output; theft of data / information; unauthorized copying of output; unauthorized visibility of documents; unauthorized printing and distribution of information; directing prints and distributing information to people who are not entitled to receive it; and handling sensitive documents to non-security cleared personnel for shredding. Those security threats are mainly related to the CAIS output security.

It is also observed that almost all the previous studies in CAIS security threats research area have been implemented in developed countries; and according to the author's knowledge no empirical research has examined CAIS security threats in developing countries. It is believed that conducting the current study in a developing country, Saudi Arabia, could thus yield significant results and bridge the gape in this research area.

3.1 The research hypotheses

The current research attempts 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.

3.2 The research methodology

In the current study 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 the current study, 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 Jubeel. 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.

In the questionnaire, the respondents were asked to indicate the frequency of occurrence of each security threat by ticking one among five available choices (less than once a year; once a year to monthly; once a month to weekly; one a week to daily; and more than once a day or more frequently). Reliability test has been carried out on the questionnaire using the Alpha Cronbach model, to explore its internal consistency, based on the average inter-item correlation. The result of the reliability test shows that the questionnaire design is highly reliable, and the collected data related to the frequency of

occurrence of CAIS security threats in Saudi organizations are highly reliable and consistent (Alpha = 0.8627).

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 (Kruskal-Wallis test) had been used to investigate and test the research hypotheses. Non-parametric tests - rather than parametric tests - are the most appropriate statistical tests for analyzing data collected in this research since these tests are "distribution free" and do not require normal distribution of data; and can efficiently deal with small samples. Non-parametric tests are also very suitable to analyze nominal, ordinal, categorical, and scale ranked data (See: Dickinson, 1990; Miller, 1991; Hessler, 1992; Melville and Goddard, 1996; Wackerly et al., 1996; and Abu-Musa 2003b). 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.

3.3 The research results

The research has a representative and unbiased research sample. One hundred and thirty six 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 (Fig. 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.

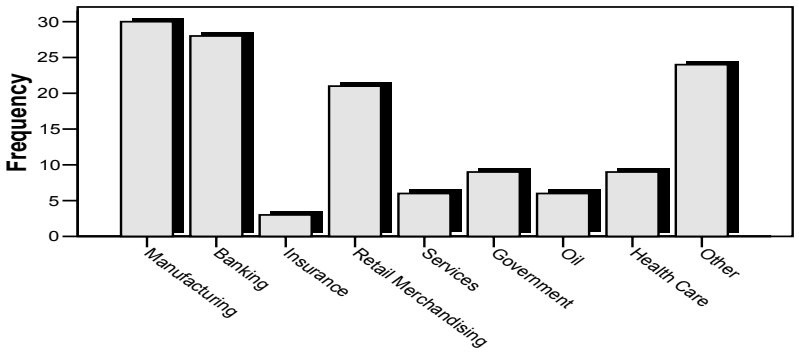

Fig. 1. Responded businesses.

As Fig. 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 (Fig. 2).

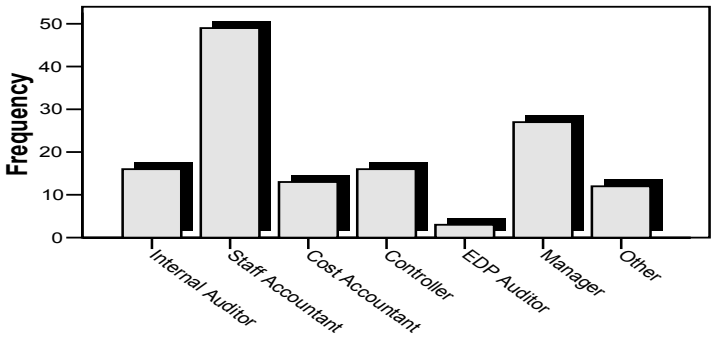

Fig. 2. Respondents' job titles.

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 (Fig. 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. The obtained results from this study were consistent with the results of the previous studies carried out in this area (See: Doost, 1990; Rockwell, 1990; Meall, 1992; Feeney, 1993; EDPACS, 1992; Mau and Catlin, 1993; Corbitt, 1996; Moss, 1996; KPMG, 2000; Green, 2003; and Swann, 2004).

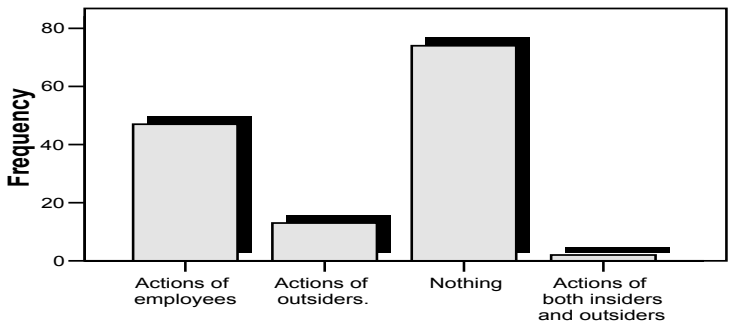

Fig. 3. Security financial losses.

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

3.3.1 Accidental entry of bad data by employees

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 result provides an indicator of the high frequency of accidental entry of bad data by employees in Saudi organizations.

3.3.2 Intentional entry of bad data by employees

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 six 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 above results suggests that the frequency of occurrence of intentional entry of bad data by employees quite high in the Saudi organizations.

3.3.3 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.

3.3.4 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.

3.3.5 Unauthorized access to the data and / or system by employees

The findings revealed that 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.

3.3.6 Unauthorized access to the data and / or system by outsiders

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.

3.3.7 Employees' sharing of passwords

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.

3.3.8 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.

3.3.9 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.

3.3.10 Introduction (entry) of computer viruses to the systems

The statistical results reported that 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, introduction of computer viruses seems to be a frequent security threat in the Saudi organizations. The possible reasons might be that anti-virus utility programs were not installed; not be updated on a regular basis to enable detection of newer viruses. Anti-virus software might not be set to automatically scan computer files when the system is first turned on. Employees might not be trained well to scan any external media they introduce to the system during the daily activities.

3.3.11 Suppression or destruction of output

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.

3.3.12 Creation of fictitious / incorrect output

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.

3.3.13 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.

3.3.14 Unauthorized copying of output

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.

3.3.15 Unauthorized document visibility

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; and 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.

3.3.16 Unauthorized printing and distribution of data / information

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.

3.3.17 Directing prints and distributed information to people not entitled to receive

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.

3.3.18 Sensitive documents are handed to non- security cleared personnel for shredding

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.

3.3.19 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 results provide an evidence of the low frequency of interception of data transmissions from remote locations in the Saudi organizations

4. Discussion of the Results

As automated accounting systems become more readily available to all types and sizes of businesses, the need to understand and employ adequate systems security becomes an issue no business can ignore. Katz (2000) argued that maintaining security is a never-ending struggle. Just when one has an airtight system in place, a new hacker technology or an especially diabolical adversary enters the picture.

The results also revealed 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 provide further evidence that the big security headaches are now perceived to come from within, not outside. The organization's own employees are potentially its own worst enemies, posing the most serious risk to security (Loch et al., 1992; Davis, 1996; Weingartner and Burton, 1991; Jenkins et al., 1992; Schultz, 2002; Carnevale, 3003; Green, 2003; and Swann, 2004).

The obtained results are consistent with the opinion of the Organization for Economic Co-operation and Development (OECD) (1992) stating that employees who have been granted authorized access to the system might pose a larger threat to information systems. They might be honest, well-intentioned employees who, owing to fatigue, inadequate training or negligence, commit an inadvertent act that deletes massive amounts of data. They may be disgruntled or dishonest employees who misuse or exceed authorized access to tamper deliberately with the system for their own enrichment or to the detriment of the organization.

Smith (1995) confirmed that "creating a secure environment is complicated by the fact that workers must support security efforts for them to be effective, but it is often employees that pose the greatest threat to security. Most workers, however, are not actively trying to breach security. Often, careless mistakes and indiscriminate access to information are at the root of security problems. Therefore, the more informed users are, the more likely they are to accept the policies". Again, Wood and Banks (1993) stated that human errors is one of the major and most serious threats to information security that is often ignored or dismissed with statements such as "it's inevitable" or "there is not much we can do about it". This type of thinking runs counter to reality, since studies have shown that, of all systems threats, human error has the highest probability of occurring.

The previous studies also indicated that, with the right professional assistance, human errors could be easily corrected or significantly reduced. According to Haugen and Selin (1999) unintentional acts, while costly at times, could be corrected or avoided through training and supervision.

Intentional acts such as entry of bad data, destruction of data, introduction of computer viruses, generally fall into the designation of computer crime. These crimes might be acts of sabotage intended to destroy the CAIS components or acts of computer fraud where the intent is to steal money, data, computer time and/or services. They would also include manipulative activities such as deleting or altering records and files to remove damaging information or create false information. However, according to the results of the current study, intentional entry of bad data by employees seems to be a low-level security threat in the Saudi organizations. Intentional entry of bad data is more likely associated with computer crimes such as computer fraud. However, there are many possible reasons behind committing computer crimes such as embezzlement and computer fraud. According to Haugen and Selin (1999) employees might commit such computer crimes and steal from the business for which they work, the more common reasons being revenge, overwhelming personal debt, substance abuses and lack of internal controls. Business today is very competitive, and employees can feel much stressed. As a result, they have feelings of being overworked, underpaid and unappreciated. If employees are also struggling with serious personal problems, their motivation to commit fraud may be quite high.

The results tend to provide an evidence of consistent perception regarding the significance CAIS security threats across Saudi organizations. The results of the Kruskal-Wallis test (Appendix 2) showed no significant differences among different Saudi organizations regarding the frequency of occurrence of CAIS security threats, except for accidental and intentional destruction of data by employees (at significance level $p = 0.05$). It is also observed that banks and financial institutions as well as other organizations which offer internet services reported higher perception of the occurrence of such security threat comparing to other organizations.

5. 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. Accordingly, it is recommended to strength the implemented security controls over the weak point to provide a better protection to CAIS against these perceived security threats.

The results of Kruskal-Wallis test show that there are no significant differences between different organizations' types regarding the frequency of occurrence of CAIS security threats in the Saudi environment (except for accidental and intentional destruction of data by employees). 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

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

[2] Abu-Musa, A. 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.

[3] Anderson, R. J. (1996), "From Critics to Coaches", *Bank Management,* (May / Jun.), pp. 26-32.

[4] Carnevale, W. (2003), "Awareness of Computer-Security Threats Is Still Inadequate", *Chronicle of Higher Education*, (Vol. 50, Iss. 12), pp. 30 - 32.

[5] Coffin, R. G. and C. Patilis (2001), "The Internal Auditor's Role in Privacy", *Internal Auditing,* Mar/Apr., (Vol.16, Iss.2), PP. 22-28.

[6] Collier, P., R. Dixon and C. Marston (1991), "The Role of Internal Auditor in the Prevention and Detection of Computer Fraud", *Public Money and Management,* winter, pp. 53 - 61.

[7] Corbitt, T. (1996), "Stop, Thief", *Accountancy Age*, (Feb), p. 20

[8] Dhillon, G. (1999), "Managing and controlling computer misuse", *Information Management & Computer Security,* (Vol. 7, Number 4), PP. 171-175.

[9] Doost, R. K. (1990), "Accounting Irregularities and Computer Fraud", *National Public Accountant,* (Vol. 35 Iss. 5), pp. 36 - 39.

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

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

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

[13] Dickinson (1990), *Statistical Analysis in Accounting and Finance*, Philip Allan, London.

[14] EDPACS (1992), "A major International Organization Ignores Computer Security", *EDPACS: The EDP Audit, Control, & Security Newsletter,* (Vol. 20, Iss. 4), pp. 18-19.

[15] Feeney, K. (1993), "How to Deal with Computer Fraud", *Connecticut CPA Quarterly*, (March), pp. 10-11.

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

[17] Green, M. (2003), "Securing the System", *Best's Review*, (Vol. 103, No. 10), pp. 80 - 84.

[18] Grundy, E., Collier, P. and S., Barry (1994), "Auditing Personnel: A Human Resource Approach to Information System Control", *Managerial Auditing Journal,* (Vol. 9), pp. 10-16.

[19] Haugen S. and J. R. Selin (1999), "Identifying and Controlling Computer Crime and Employee Fraud", *Industrial Management and Data Systems,* (Vol. 99, Iss. 8).

[20] Hessler R. M, 1992, Social Research Methods, West Publishing Company, New York, USA.

[21] Hermanson, D. R.; M. C. Hill; and D. M. Ivancevich, (2000) "Information Technology-Related Activities of Internal Auditors", *Journal of Information Systems*, (Supplement, Vol. 14, Issue 1), pp. 39-53.

[22] Hood, K. L. and J. 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.

[23] Hunton, J.; A. Wright; and S. Wright, (2005) "Business and Audit Risks Associated With ERP Systems: Knowledge Differences between Information Systems Audit Specialists and Financial Auditors", *Journal of Information Systems*, Forthcoming.

[24] Jenkins, B., P. Cooke and P. Quest (1992), *An Audit Approach to Computers,* Institute of Chartered Accountants In England And Wales, London.

[25] Katz, D. (2000), "Elements of a Comprehensive Security Solution", *Health Management Technology,* (Vol. 21, Iss. 6), pp. 12-16.

[26] KPMG (2000), *Information Security Survey 2000, Executive Summary*, April, KPMG, London.

[27] Leinicke, L. M.; W. M. Rexroad and J. D. Ward (1990), "Computer Fraud Auditing: It Works", *Internal Auditor,* (Vol. 47 Iss. 4), pp. 26 - 33.

[28] Levi, P. (1993), "PC security for accountants - What's Hot and What's New", *Accounting Technology,* (Feb. / Mar.), pp. 26-30.
[29] Loch, K. D., Houston H. C. and M. E. Warkentin (1992), "Threats to Information Systems: Today's Reality, Yesterday's Understanding", *MIS Quarterly,* (June), pp. 173 - 186.
[30] Mclean, G. (2000), "The New Age of Bank Security", *Canadian Banker*, (Vol. 107, Iss. 4), pp. 14 - 19.
[31] Mau, S. and J. Catlin (1993), "Systems Security in 90's", *Interpreter*, (January), pp. 8-9.
[32] Meall, Lesley (1992), "Computer Crime: Foiling the Fraudsters", *Accountancy,* (November), pp. 56-57.
[33] Melville S and W. Goddard (1996) *Research Methodology: An Introduction for Science and Engineering Students*, Juta and Co. Ltd, Kenwyn.
[34] Miller, D. C. (1991) *Handbook of Research Design and Social Measurement,* (Fifth Edition), SAGE Publications, London.
[35] Moss, N. (1996), "Banks at Mercy of Hackers", *The European*, October 10, N.335, p. 24.
[36] 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
[37] National Institute of Standards and Technology (2003), Computer Security Division, Information Technology Laboratory, *Standards for Security Categorization of Federal Information and Information Systems,* Initial Publication Draft, Version 1.0, May.
[38] OECD (Organization for Economic Co-operation and Development) (1992), *Guidelines for the Security of Information Systems*, The Council of the OECD, 26 November.
[39] Parker, D. B. (1976), *Crime By Computer,* Charles Scribner's sons, New York.
[40] Qureshi, A. A. and J. G. Siegel (1997), "The Accountant And Computer Security", *The National Public Accountant,* Washington, May, (Vol. 43, Iss. 3), pp. 12-15.
[41] Rockwell, R. (1990), "The Advent of Computer Related Crimes", *Secured Lender*, (Jul /Aug), pp. 40 - 42
[42] Roufaiel, N. S. (1990), "Computer Related Crimes: An Educational And Professional Challenge", *Managerial Auditing Journal,* (Vol. 5, Iss. 4), pp. 18 - 25.
[43] 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.
[44] Schultz, E. E. (2002), "A Framework for Understanding and Predicting Insider Attacks", Computers & Security, (Vol. 21, Iss. 6), pp. 256 – 531.
[45] Schweitzer, J. A. (1987), *Computers, Business, and Security,* Butterworth Publishers, London.
[46] Siponen, M. T. (2000), "A conceptual Foundation for Organizational Information Security Awareness", *Information Management and Computer Security*, Bradford, (Vol. 8, Iss. 8), PP. 31- 44.
[47] Smith, L. B. (1995), "On The New Beat", *PC Week,* (October30) (Vol. 12, No. 43), pp. E1-2.
[48] Swann, J. (2004), "Always on the Case: Engaging your Staff in Bank Security", *Community Banker*, (March, Vol. 13, Iss. 3), pp. 44 - 47.
[49] United States General Accounting Office (GAO) (2003), *Information Security: Computer Controls over Key Treasury Internet Payment System*, Report to Congressional Requesters, July.
[50] Wackerly, D. D., W. Mendenhall and R. L. Scheaffer, (1996) *Mathematical Statistics with Applications,* Duxbury Press, Wadsworth Publishing Company, London.
[51] Warren, M. J. (2002), Security practice: survey evidence from three countries, *Logistics Information Manageme,* (Vol. 15, Iss. 5/6), PP. 347-351.
[52] Weingartner, A. and M. Burton (1991), "PC Security - Don't Be Caught Out", *Computer Security Guide,* pp. 33 - 35.
[53] White, Gayle Webb and Sheila J Pearson (2001), "Controlling corporate e-mail, PC use and computer security"; *Information Management & Computer Security*, Vol. 9, Iss. 2/3; pp. 88-93.
[54] Williams, P. (1995), "Safe, Secure And Up To Standard", *Accountancy,* p. 60.
[55] Wood, C. C. and W. W. Banks (1993), "Human Error: An Overlooked but Significant Information Security Problem", *Computers & Security*, (Vol. 12, Iss. 1), pp. 51 - 60.

[56] Wright, S. and A. Wright (2002), Information system assurance for enterprise resource planning systems: Implementation and unique risk considerations, *Journal of Information Systems*, Vol. 16, Supplement, pp. 99-113.

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 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.
7. In the last year, the accounting system has: (Please, tick)
   - ❒ Suffered a loss due to the security breach actions of employees.
     Specify the loss value .....
   - ❒ Suffered a loss due to the security breach actions of outsiders.
     Specify the loss value .....

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 frequently
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					
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

Frequencies of CAIS Security Threats & The Results of Statistical Tests

Computerized Accounting Information Systems (CAIS) Security Threats	Frequencies of CAIS Security Threats						Kruskal-Wallis Test	
	Never	Less than once a year	Once a year to monthly	Once a month to weekly	Once a week to once a day	more than once a day	Chi - Square	Sig.
1. Accidental entry of bad data by employees	2 (1.5%)	25 (18.4%)	47 (34.6%)	27 (19.9%)	30 (22.1%)	5 (3.7%)	8.008	.433
2. Intentional entry of bad data by employees	14 (10.3%)	67 (49.3%)	31 (22.8%)	14 (10.3%)	6 (4.4%)	4 (2.9%)	10.748	.216
3. Accidental destruction of data by employees	13 (9.6%)	51 (37.5%)	40 (29.4%)	25 (18.4%)	6 (4.4%)	1 (.7%)	15.009	.059
4. Intentional destruction of data by employees	17 (12.5%)	81 (59.6%)	22 (16.2%)	12 (8.8%)	3 (2.2%)	1 (.7%)	15.290	.054
5. Unauthorized access to the data / system by employees	15 (11%)	92 (67.6%)	14 (10.3%)	13 (9.6%)	2 (1.5%)	0	8.474	.389
6. Unauthorized access to the data and / or system by outsiders (hackers)	17 (12.5%)	94 (69.1%)	14 (10.3%)	4 (2.9%)	4 (2.9%)	0	5.771	.673
7. Employees' sharing of passwords	13 (9.6%)	60 (44.1%)	26 (19.1%)	12 (8.8%)	13 (9.6%)	12 (8.8%)	2.649	.954
8. Natural disaster such as fire, flooding, loss of power	14 (10.3%)	97 (71.3%)	17 (12.5%)	1 (.7%)	4 (2.9%)	3 (2.2%)	8.367	.398
9. Human- made disasters such as fire, loss of power	14 (10.3%)	96 (70.6%)	18 (13.2%)	2 (1.5%)	3 (2.2%)	3 (2.2%)	5.677	.683
10. Introduction of computer viruses to the system	13 (9.6%)	71 (52.2%)	30 (22.1%)	12 (8.8%)	7 (5.1%)	3 (2.2%)	8.169	.417
11. Suppression or destruction of output	15 (11%)	81 (59.6%)	19 (14%)	13 (9.6%)	3 (2.2%)	5 (3.7%)	7.569	.477
12. Creation of fictitious / incorrect output	13 (9.6%)	75 (55.1%)	29 (21.3%)	10 (7.4%)	7 (5.1%)	2 (1.5%)	12.381	.135
13. Theft of data / information	13 (9.6%)	95 (69.9%)	12 (8.8%)	8 (5.9%)	4 (2.9%)	4 (2.9%)	10.723	.218
14.Unauthorized copying of output	15 (11%)	91 (66.9%)	18 (13.2%)	4 (2.9%)	4 (2.9%)	4 (2.9%)	6.998	.537
15. Unauthorized document visibility of output	9 (6.6%)	80 (58.8%)	22 (16.2%)	12 (8.8%)	8 (5.9%)	5 (3.7%)	4.886	.770
16. Printing and distribution of information by unauthorized persons.	14 (10.3%)	82 (60.3%)	23 (16.9%)	8 (5.9%)	4 (2.9%)	5 (3.7%)	5.383	.716
17. Directing prints and distributing information to un-entitled people	11 (8.1%)	75 (55.1%)	30 (22.1%)	11 (8.1%)	1 (.7%)	8 (5.9%)	8.280	.407
18. Handling Sensitive documents to non-security cleared personnel for shredding.	12 (8.8%)	83 (61%)	26 (19.1%)	6 (4.4%)	5 (3.7%)	4 (2.9%)	7.769	.456
19. Interception of data transmissions from remote locations	15 (11%)	81 (59.6%)	24 (17.6%)	8 (5.9%)	2 (1.5%)	6 (4.4%)	7.342	.500

مخاطر أمن نظم المعلومات المحاسبية الإلكترونية دراسة ميدانية على المنشأت السعودية*

أحمد عبد السلام أبو موسى
قسم المحاسبة ونظم المعلومات الإدارية
جامعة الملك فهد للبترول والمعادن

(قدّم للنشر في ٢٠٠٤/٠٥/٢٢م؛ وقبل للنشر في ٢٠٠٥/٠٥/٢٠م)

ملخص البحث. يهدف هذا البحث إلى التعرف على وإختبار المخاطر الرئيسية والهامة التي تهدد أمن نظم المعلومات المحاسبية الإلكترونية في المنشأت السعودية. ولقد قام الباحث بعمل دراسة ميدانية على المنشأت السعودية مستخدماً فى ذلك قائمة إستقصاء معدة خصيصاً لهذا الغرض. ولقد أوضحت نتيجة الدراسة أن كثيراً من المنشأت التى شاركت فى الدراسة قد عانت من وجود خسائر مالية كبيرة بسبب التعديات على أمن نظم المعلومات المحاسبية بواسطة أشخاص من داخل وخارج تلك المنشأت. وتشير نتائج الدراسة أن أهم المخاطر التى تهدد أمن نظم المعلومات الإلكترونية فى المنشأت السعودية تمتثل فى الإدخال المتعمد وغير المتعمد لبيانات غير سليمة وكذلك التدمير غير المتعمد للبيانات من قبل موظفى المنشأة. كما يعد إشتراك موظفى المنشأت فى إستخدام نفس كلمات السر؛ وإدخال فيروسات إلى النظام المحاسبى؛ وتدمير أو طمس بعض مخرجات النظام المحاسبى؛ والكشف عن بعض المعلومات الهامة لإشخاص غير مرخص لهم بالإطلاع عليها؛ وكذلك توجيه بعض مخرجات الحاسب الألى إلى اشخاص غير مخول لهم بإستلامها والإطلاع عليها من المخاطر الهامة التى تهدد أمن نظم المعلومات الإلكترونية فى المنشأت السعودية. ومن ثم تبدو الحاجة ملحة لتدعيم الضوابط الرقابية على نقاط الضعف فى نظم الرقابة الداخلية المتعلقة بتلك المخاطر. وكذلك زيادة الوعى داخل المنشأت

* تم إجراء هذا البحث بتمويل من كلية الإدارة الصناعية– جامعة الملك فهد للبترول والمعادن– المملكة العربية السعودية.

السعودية فيما يتعلق بأمن نظم المعلومات المحاسبية الإلكترونية لكى توفر الحماية الازمة والكافية ضد المخاطر الحالية والمحتملة التى تهدد أمن تلك النظم.