J. King Saud Univ., Vol. 18, *Comp. & Info. Sci*., pp. 67-101 (A.H. 1426/2006)

Evaluating the Security Controls of CAIS in Saudi Organizations: An Empirical Study

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

(Received 8 October 2005; accepted for publication 8 April 2006)

Abstract. This paper examines the existence and adequacy of implemented Computerized Accounting Information Systems (CAIS) security controls to prevent, detect and correct security breaches in Saudi organizations. An empirical survey, using a self-administered questionnaire, was carried out to achieve this purpose. Five hundred questionnaires were distributed on a random sample of Saudi organizations. Two hundred and seventy five valid, usable questionnaires were collected and analyzed. The results of the study highlight a number of inadequately implemented CAIS security controls, and some suggestions and recommendations are introduced to strengthen the weak points and to close the loopholes in the present CAIS security controls in Saudi organizations. From a practical standpoint, managers, auditors, IT users and practitioners alike stand to gain from the findings of this study. The results could enable them to better understand and secure their CAIS and to champion IT development for the success of their businesses.

Key Words: Security controls; CAIS; empirical study; developing countries; and Kingdom of Saudi Arabia.

1. Introduction

Information has become one of the most valuable assets for most organizations. Business survival and success are heavily dependent upon the accuracy, integrity and continued availability of critical information. The reliance on information and continuous changes in technology force organizations to implement security controls to protect their Computerized Accounting Information Systems (CAIS) against potential security threats. However, the failure to secure the CAIS and the information they contain or to make it available when it is required can, and does, lead to great financial and non-financial losses. It is argued that individuals who are more aware of the potential security threats against their CAIS would be more sensitized to the dangers of inadequate security controls and would more likely feel that their CAIS security is unsatisfactory.

However, many organizations do not realize the importance of CAIS security until some unauthorized access to their systems occurs or modification, alteration or destruction of their critical files has happened. Organizations can no longer disregard the importance of information security in the light of computer fraud, hackers and computer viruses. Accordingly, the need to understand and employ adequate security controls over CAIS has become an issue no business can ignore [3, 4, 11, 16, 26, 29, 30, 31, 38].

The Kingdom of Saudi Arabia, the largest country in the Middle East and the 12th largest in the world, measuring approximately 2.2 million square km, has been selected as the location in which to conduct the current survey. It also has the largest gross domestic product (GDP) in the Middle East. Saudi Arabia is an oil-based economy, having the largest reserves of petroleum in the world (26 percent of the proven reserves), ranks as the largest exporter of petroleum, and plays a leading role in OPEC. The kingdom has launched a wave of cautious economic reforms aimed among others, at diversifying its oil-based economy and joining the WTO, which is evidence of its efforts to succeed in the fast approaching era of global integration [27, 39]. Saudi Arabia has a dynamic interaction between traditional culture and modern economic and business realities, which make Saudi Arabia a unique culture [49] in which to implement the current study.

The Kingdom of Saudi economy can be considered as a "one-crop economy," which relies basically on oil exports for its revenues. However, there is a dramatic shift in the economy of Saudi Arabia. While the phenomenal boom experienced by the Saudi economy came to its standstill during the Gulf War, the economy managed to regain its strength recently, and it is expected to be one of the strongest economies in the world. Several commodities ranging from fertilizer to pipes to furniture are produced in plants located at various industrial estates throughout the Kingdom. In order to remain competitive, computerization has become a necessity rather than a luxury for these manufacturers. Furthermore, service organizations need computerization more than ever before to improve their performance, satisfy their customers' needs, and to reduce operating costs without compromising service quality [12, 47, 48, 49].

It is argued that while Saudi Arabia is rich in capital, it has had and continues to have an inadequate local supply of computer specialists. In an attempt to close the supply-demand gap in native computer specialists, and to acquire the contemporary computer know-how, over the years Saudi students were sent abroad (particularly to the United States) to obtain their education and to bridge the gap of a good domestic supply of computer specialists. In spite of this, Saudi computer and IT education is still not coping with an increasing demand for computer professionals [12, 49]. Recently however, the education authorities responsible for higher education have moved to reconsider the curriculum to meet business demands for more graduates who can cope with global business changes [5].

The main objective of this study is to investigate and evaluate the existence and adequacy of implemented CAIS security controls in Saudi organizations in order to prevent, detect and correct CAIS security breaches. The current study also aims to investigate if there are significant differences among Saudi organizations regarding the implemented CAIS security controls.

An empirical survey has been carried out on a random sample of Saudi organizations, using a self-administered questionnaire, to achieve the research objectives. The current study is an attempt to investigate the following two research questions:

- Are there adequate security controls implemented to protect CAIS against the perceived security threats in Saudi organizations?
- Are there significant differences among Saudi organizations regarding implemented CAIS security controls?

The remainder of this paper is organized as follows. The second section presents the literature review and previous studies related to security controls of CAIS. This is followed by the statement of research hypotheses. The study's research method is then described. This is followed by the presentation and analysis of the study's major empirical results. The final section of this paper provides conclusions and recommendations for further research.

2. Literature Review

A review of the literature reveals diverse views regarding the classification of CAIS security controls. Security controls of CAIS could be classified according to their ***purpose:*** to deter, prevent, detect and correct security threats. The objective of deterrent security controls is to create an atmosphere of control compliance, while preventative security controls should be designed to reduce the possibility of an attack. Once a system has been violated, detective controls could help in identifying the occurrence of harm and security breaches. Corrective controls serve to reduce the impact of the threat after a loss has occurred. Thus, the purpose of corrective controls is to aid in recovery from damage or in reduction of the harmful effects of its occurrence [3, 37].

Security controls can also be categorized according to their association with the data ***processing stages:*** e.g. input, processing, storing and output security controls. The purpose of input controls is to ensure that each transaction is authorized, processed correctly and processed only once. Processing controls should be used to ensure that transactions entered into CAIS are valid and accurate, that external data are not lost or altered and that invalid transactions are reprocessed correctly. Output security controls

are used to ensure that no unauthorized copies of output were made, and that the printouts are directed only to authorized individuals. Storage security controls ensure that all stored data and programs are secured against unauthorized access, manipulation, alteration and disclosure. Alternatively, security controls could also be classified according to their ***nature***, including for example, organizational, physical access, data and data integrity, software, off-line programs and data security controls.

Reviewing the literature reveals a paucity of studies concerned with evaluating the security controls of CAIS in developing countries, which represents a relatively new area for research. Boockholdt [6] examined the impact on computer security and data integrity of linking personal computers in user departments with the corporate mainframe computer. Eighty-five Certified Information Systems Auditors were surveyed to investigate their views regarding data security and integrity. The results of the study reveal that access and physical security controls, data backup and maintenance of hardware have become critical. Security classification of data should be established and different access restrictions for each classification should be implemented. Many of these security controls are included in our proposed CAIS security controls checklist to be tested in Saudi organizations [6].

Buttross and Ackers [7] discussed microcomputer security exposure and microcomputer organizational, hardware, software and data security controls. They introduced a proposed security controls checklist that could be used to help internal auditors in identifying and correcting their CAIS security exposures through evaluating the security controls. The checklist included the following security control categories: organizational controls, hardware controls, software controls, and data and data integrity controls. The checklist was mainly designed for small and medium-sized organizations. Again, a selected number of security controls introduced by Buttross and Ackers [7] were incorporated in our proposed checklist to be empirically investigated in the Saudi environment.

Collier et al. [9] conducted research to explore how public service organizations assign responsibility for the prevention and detection of computer fraud. The results of the study revealed that most respondents considered that the specific responsibility for countering computer fraud was not consistently attributed within their organizations. Respondents mentioned that the information services function most commonly held the responsibility for computer fraud prevention and detection. However, 56 percent of the respondents considered the internal audit departments to be responsible for detecting and preventing computer fraud.

In 1992, the Committee of Sponsoring Organizations (COSO) Report [10] introduced a framework for the consideration of control risks, which expanded the focus of the traditional view of controls at the detailed account and assertion level to include a

global business perspective. The COSO framework was integrated into SAS 55 (1988) and 78 (1995). These standards direct the auditor to consider the broader business and control risks of a company, which can have a direct impact on potential misstatements in the financial statements or on appropriate disclosures [10].

The IT Governance Institute (ITGI) and the Information Systems Audit and Control Foundation (ISACA) [25] developed the Control Objectives for Information and Related Technology (COBIT). COBIT provides managers, auditors, and IT users with a set of generally accepted IT control objectives to assist them in maximizing the benefits derived through the use of IT and developing the appropriate IT governance and control in their organizations. The first edition of COBIT was published in 1996, the second edition in 1998, the third edition in 2000, and the on-line edition became available in 2003. COBIT incorporates generally applicable and accepted international standards for good practice of IT management and control. Many of the COBIT security controls were selected and incorporated in the proposed checklist to be empirically tested in the Saudi business environment.

ISO 17799 also introduces a comprehensive set of controls comprising best practices in information security. It is a recognized generic international information security standard. ISO 17799 was originally published in the early 1990's as the "DTI Code of Practice", by the Department of Trade & Industry in the UK. In 1995, it was further developed and published as BS 7799 by the British Standards Institute, which was updated again in 1999. The original BS 7799 was revised and reissued in September 2002 [23, 24].

The ISO 17799 standard is comprised of ten main sections: security policy, system access control, computer & operations management, system development and maintenance, physical and environmental security, compliance, personnel security, security organization, asset classification and control, and business continuity management. Many of the security controls were also selected and incorporated in the proposed security controls checklist to be empirically investigated in the Saudi organizations.

In December (2000), the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) established a joint technical committee named ISO/IEC. The committee developed and published the ISO/IEC 17799:2000 (The Code of Practice for Information Security Management), which is now considered as the international standard and the best practice for implementing security management. The standard was published in 2000 in its first edition, and updated in June 2005 [23, 24].

Dougan [17] suggested an alternative internal control checklist for computer systems. This checklist could be used to check security controls in place and to ensure

that the implemented security procedures are adequate and effective to prevent computer data losses and security breaches. Dougan [17] grouped the security controls under four main categories, namely: computer room site (physical security), documentation, maintenance, and protection of data. According to Dougan, the suggested security checklist could be useful for those who have nothing; and for others it may serve as a prod to recheck their internal controls [17].

Solms [40] has addressed the general background regarding CAIS security evaluations and has discussed the scope and responsibility for information security. His paper discusses a number of information security evaluation schemes and certification techniques, such as: Trusted Security Evaluation Criteria schemes, ISO 9000 (BS 570), the Code of Practice for Information Security Management, BS 7799, and Self Evaluation of Security Techniques.

Henry [19] surveyed 261 companies in Hampton Roads, Virginia, USA, to determine the nature of their accounting systems and security in use. Henry [19] discussed and tested the following seven CAIS security methods: encryption, password access, backup of data, virus protection, authorization for system changes, physical system security, and periodic audits. The results of Henry's survey [19] indicate that 80.3 percent of the companies backup their accounting systems. 74.4 percent of the companies secure their accounting system with passwords, but only 42.7 percent utilize protection from viruses. Physical security and authorization for changes to the system are employed by less than 40 percent of the respondents. The survey results also show that only 15 companies use encryption for their accounting data. Almost 45 percent of the sample underwent some sort of audit of their accounting data. Selected security controls were incorporated in our proposed security controls checklist to be empirically investigated in Saudi Arabia.

Qureshi and Siegel [37] discussed the responsibility of accountants regarding assuring the security of CAIS. The paper discussed the anticipated physical access and communication security controls, which include deterrent controls, preventive controls, detective controls, input controls and processing security controls. Many of the security controls introduced by Qureshi and Siegel [37] are selected to be empirically tested in the Saudi environment.

Hood and Yang [21] studied the security of banking information systems in China. The results revealed that management was aware of security but the respondents believed that their banks had not taken enough action to reduce the potential risks and losses due to the lack of financial and human resources. Concerning security controls, two thirds of the respondents believed that their banking system could be protected from internal attack, while less than half were not confident about external attacks. Moreover,

it seems that passwords, daily backups, and monitoring of network activities were the most common security controls in the Chinese banking system.

The National Institute of Standards and Technology (NIST) [34] issued the "Generally Accepted Principles and Practices for Securing Information Technology Systems." The document provides a baseline that organizations can use to establish and review their information technology security programs. Management, internal auditors, users, system developers, and security practitioners could use the guideline to gain an understanding of the basic security requirements most information technology systems should contain. In 1998, NIST [35] also issued the guide for developing security plans for information technology systems to improve protection of information technology resources. The purpose of the security plan was to provide an overview of the security requirements of the CAIS and to describe the controls in place or planned for meeting those requirements. The security plan also delineates responsibilities and expected behavior of all individuals who access CAIS.

Zviran and Haga [50] carried out an empirical study to evaluate password security as one of the most common control mechanisms for authenticating users of CAIS. The study investigated the core characteristics of user-generated passwords and the associations among those characteristics. The results of the study revealed that despite the widespread use of passwords, little attention has been given to the characteristics of their actual use. The results also revealed that almost 50 percent of the users surveyed in this study reported passwords composed of five or fewer characters, the vast majority of respondents use only alphabetic characters and never changed their password. The findings also highlight the need to investigate the effectiveness of educational efforts to raise the security consciousness of system users.

Dhillon [14] argued that many of the losses resulting from computer-related fraud could be avoided if organizations adopted a more pragmatic approach to dealing with such incidents. The paper encourages organizations to adopt a balanced approach to security controls which places equal emphasis on technical, formal and informal interventions against their computerized systems in order to minimize the losses of computer fraud.

In 2000, the public oversight board (POB) [37] discussed the issue of unique risks and controls posed by increasingly sophisticated information processing systems. The board encouraged auditors to expand their knowledge of new business-oriented information systems, as such knowledge would facilitate the development of more effective audit approaches. The POB also recognized the need of attracting and retaining qualified technology specialists for audit support.

Dhillon and Backhouse [15] discussed the confidentiality, integrity, availability, responsibility, trust and ethicality principles as key factors for successful management of information security in the next millennium. Again, the paper recommended paying equal attention to technical and organizational security controls in designing and evaluating CAIS.

Siponen [41] introduced a conceptual foundation for organizational information security awareness programs to minimize end-user errors and to enhance the effectiveness of implemented CAIS security controls. Siponen [41] emphasized the importance of information security awareness. He argued that prescribed information security techniques or procedures would lose their real usefulness if they were misused, misinterpreted, not used, or not properly implemented by end-users.

Detecting and preventing unauthorized access to CAIS by internal and external parties has become an important issue. The results of Furnell and Dowland's [18] study revealed that traditional methods of user authentication and access security control do not provide comprehensive protection and offer opportunities for compromise by various classes of abuse.

Coffin and Patilis [8] studied the role of internal auditors in evaluating the security controls for protecting sensitive data in financial institutions such as banks, security firms, and insurance companies. They argued that internal auditing could significantly help organizations in determining and evaluating the implemented CAIS security controls as well as compliance with applicable regulations.

White and Pearson [45] surveyed over two hundred US companies to investigate the security controls related to the 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 companies began to use computer technology before implementing appropriate safeguards; and the majority of the companies' safeguards continued to be lacking.

Warren [44] carried out a survey to investigate the security practices of computerized information systems in three countries: Australia, the U.K. and the U.S.A. The paper attempted to evaluate security practices from different perspectives and to investigate whether the security practices varied from one country to another. The results of the survey revealed that:

- In Australia, poor levels of computer security were found among Australian organizations. Many of the security problems were identified as implementation of poor security procedures. The results also indicated that 45 percent of organizations do not budget for computer security.

- In the U.K., 42 percent of organizations did not have an information security policy. The findings also revealed that 49 percent of the organizations listed budget constraints as being an issue in implementing computer security.
- In the U.S.A., theft of information and financial fraud cause 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 U.S. security practices seem to be more effective than those of Australia or the U.K.

Wright and Wright [46] conducted an exploratory study to obtain an understanding of the unique risks associated with the implementation of Enterprise Resource Planning (ERP) systems using a semi-structured interview approach. The research findings showed that the potential for financial statement errors and business risks were intensified as a result of the lack of proper user training. The findings also showed that ongoing risks differed across ARP applications and across vendor packages. Finally, the results suggested 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 [36] in the U.S.A. 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 CAIS. 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 than on the loss of confidentiality, integrity, or availability of information.

The United States General Accounting Office (GAO) [42] 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 the GAO review [42] revealed that although FMS and the Federal Reserve implemented numerous security controls to protect their computing resources, risks were not sufficiently assessed, and numerous security control weaknesses were identified. Accordingly, immediate actions to correct the weaknesses and to promptly address new security threats and risks as they emerge to CAIS were highly recommended.

Abu-Musa [3] carried out a survey to investigate the existence and adequacy of implemented CAIS security controls in the Egyptian banking sector (EBS). The results

of study revealed that the vast majority of Egyptian banks have adequate CAIS security controls in place. The results also revealed that the computer departments paid relatively more attention to technical security controls (such as: software and electronic access security controls, data and data entry security controls, off-line programs and data security controls, utility security controls, bypassing security controls, and user programming security controls); while internal audit departments emphasized the behavioral and organizational security controls (e.g. organizational security controls, division of duties, and output security controls). The study provides invaluable empirical results regarding inadequacies of implemented CAIS security controls, and introduces some suggestions to strengthen the security controls in the EBS.

In a recent study, Hunton et al. [22] conducted an experiment 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 ERP systems, as compared with traditional computerized (non-ERP) systems. The research findings revealed that financial auditors were significantly less concerned about ERP risks compared to IS audit specialists. Moreover, IS audit specialists were less confident in financial auditors' abilities to recognize the unique risks posed by ERP systems, which could have harmful effects on audit quality.

It is observed that most of the previous studies in the CAIS security controls research area have been carried out in developed countries, but few studies have investigated CAIS security controls issues in developing countries. It is believed that conducting this research in a developing country such as Saudi Arabia, can yield fruitful results.

It is also observed that different authors have their own research agendas regarding the security aspects of CAIS. Accordingly, CAIS security controls have been investigated in a piecemeal rather than in an integrated fashion. The current study developed and tested an integrated and comprehensive checklist of CAIS security controls. The proposed checklist could be used by any organization to conduct a self-evaluation of its CAIS security controls. The proposed checklist would help managers, internal and external auditors in identifying and correcting computer security exposures, and could enable them to evaluate the adequacy of implemented security controls. From a practical standpoint, managers and practitioners alike stand to gain from the findings of this study. The results enable managers and practitioners to better secure their CAIS and to champion information technology development for the success of their business.

3. Hypotheses

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

H_1: The implemented CAIS security controls in Saudi organizations are inadequate.

H_2: There are no significant differences among Saudi organizations regarding the adequacy of implemented CAIS security controls.

H_3: There are no significant differences among different respondent groups regarding the adequacy of implemented CAIS security controls in their organizations.

4. Methodology

In this study, an empirical survey – using a self-administered questionnaire – was conducted to investigate and evaluate the existence and adequacy of implemented CAIS security controls in Saudi organizations. The questionnaire was pre-tested on selected members of academic staff and accounting practitioners and was piloted on a selected sample of Saudi organizations. Comments and suggestions were considered in the development and revision of the final questionnaire. The questionnaire incorporated the proposed CAIS security controls check-list to be empirically investigated in Saudi organizations. The proposed checklist classified CAIS security controls under the following main security groups: organizational security controls, hardware and physical access security controls, software and electronic access security controls, data and data integrity security controls, off-line programs and data security controls, utilities security controls, bypassing of normal access security controls, user programming security controls, division of duties, output security controls, and periodic security controls.

The proposed check-list used "Yes" or "No" questions to make it easy for respondents to answer these questions and to go through the security check-list. In order to increase the respondent's motivation for completing the check-list, all questions that were similar in content and dealt with the same security control area or group were collected together under that specific security group. Also, to make it easy for respondents to answer its questions and go smoothly through the list the author meticulously considered the sequence and arrangement of the security controls in the check-list. Moreover, in deciding the order of the questions involved, the author tried to take advantage of the cognitive ties that the respondents would be likely to make among these groups.

A number of security controls countermeasures involved in the proposed security controls check-list were adopted from established research and available literature in the information security area [3, 6, 7, 9, 17, 19, 23, 24, 25, 28, 37]. Others, however, were specifically developed to meet the needs and requirements of this research. The final revised version of the questionnaire is used to survey the existence and implementation of CAIS security controls in Saudi organizations. The questionnaire is also used to collect the required information related to business and respondents profiles.

Five hundred questionnaires randomly distributed to different types of Saudi organizations (Manufacturing companies, banks, insurance companies, retail merchandising; oil and gas companies, services companies, health care, government units, and others) in seven Saudi cities: Riyadh, Jeddah, Dhahran, Dammam, Thuqba, Khubar, and Jubeel. After the follow up, three hundred and five questionnaires – representing a 61 percent initial response rate – were collected. However, 30 incomplete questionnaires were excluded from the analysis. The respondents refused to complete the

questionnaires, claiming that they contained sensitive and confidential information. After excluding the incomplete and invalid responses, the research ended with 275 valid and usable questionnaires, representing a 55 percent response rate. This response rate is considered a relatively high response rate in this kind of empirical survey.

A reliability test was 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 implemented CAIS security controls in Saudi organizations are highly reliable and consistent (Alpha = 0.8735). The Student test was carried out investigates if there were any significant differences between early responses (190 questionnaires) and late responses (85 questionnaires). The results of the Student test show no significant differences between early and late responses (at significance level p 0.05), which provides evidence of a representative and unbiased selected research sample.

The collected data show that 61 of the responding organizations were manufacturing companies and 41 were retail merchandising organizations, representing 22.2 percent and 14.9 percent of the total responses respectively (Table I). 34 respondents were banks – representing 12.4 percent of the total response. 25 respondents (9.1 percent) belonged to governmental units and 20 respondents (7.3 percent) were insurance companies. Moreover, 22 respondents (8 percent) were services organizations and 17 respondents (6.2 percent) were from the oil and gas industry. In addition, 18 respondents, representing 6.5 percent of the total belonged to health care organizations (Table I). 37 respondents (13.5 percent of the total) belonged to other organizations, e.g. hotels, car rental organizations, décor and carpentry firms, publishing and printing organizations, accounting and auditing firms, construction companies, and design organizations.

As (Table I) shows 99 respondents (36 percent) were accountants; 55 respondents (20 percent) were managers; 39 respondents (14.2 percent) were internal auditors; and 36 respondents (13.1 percent) were controllers. Moreover, 20 respondents (7.3 percent) were working as cost accountants and four respondents were EDP auditors. Again, the respondents seem to be quite representative of the job structure in Saudi organizations.

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 is performed to identify the main characteristics of the research variables. In addition, a non-parametric test (the Kruskal-Wallis test) is carried out to test the research hypotheses related to the existence and adequacy of implemented CAIS security controls in Saudi organizations. 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,” 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: 1, 2, 13, 20, 32, 33, 43].

5. Results

The statistical findings of the existence and adequacy of implemented CAIS security controls as well as the significant differences among Saudi organizations and different respondent groups will be presented and discussed in the following sections.

5.1 Organizational security controls

To explore the existence and adequacy of the implemented organizational security controls in Saudi organizations, the respondents were given an organizational security controls checklist and they were asked to indicate the controls actually implemented in their organizations. A majority of the respondents (74.5 percent) believed that their organizations' management has a serious and a positive attitude toward CAIS security. Almost two-thirds of the respondents (63.3 percent) indicated the existence and implementation of job rotation in their organizations to increase the chance of exposure of errors and irregularities. Moreover, 73.5 percent of the respondents agreed that their organizations' personnel policies include background checks to reduce the likelihood of hiring dishonest employees (Table II). Slightly more than half of the respondents (approximately 55 percent) confirmed that their organizations' employees are properly trained on their CAIS and that employees are aware of security issues; furthermore, these training programs are well documented.

On the other hand, a relatively high proportion of the respondents (almost 66 percent) believed that access to their organizations' sensitive data is not restricted to those employees who have a special need to deal with them. Moreover, slightly more than half of the respondents (54.5 percent) believed that mandatory vacations are not yet implemented in their organizations, despite knowledge that mandatory employee vacations reduce the likelihood of fraud or embezzlement and increase the chance of their exposure.

The result of the Kruskal-Wallis test (Table XII) reveals significant differences among the different Saudi organizations regarding the existence and adequacy of the implemented organizational security controls (p 0.05). Moreover, the statistical results of Kruskal-Wallis (Table XIII) show no significant differences in the opinions of different respondent groups regarding the same issue in their organizations (at significance level p 0.05).

Recommendation: According to the above results, it is recommended that measures should be taken to restrict access to organizations' sensitive data to the authorized employees with defined needs. Mandatory vacations of employees should be

taken where not already implemented. Enhanced personnel policies, including the rotation of duties, could reduce the likelihood of organizations experiencing fraud or embezzlement by increasing the chance of their exposure.

5.2 Hardware and physical access security controls

The statistical results show that the majority of the respondents (82.5 percent) believed that the theft and hazard insurance covering their organizations' computer hardware is adequate; 77.8 percent of the respondents indicated that access to their CAIS is limited and restricted to employees with defined needs (Table III).

The findings also reveal that the vast majority of the respondents (82.9 percent) reported the existence of uninterruptible power supply units to supply power during power outages. Approximately 83 percent confirmed the existence of line co-coordinators to smooth out power supply; and 79 percent of those respondents confirmed the existence of extinguishers close at hand in their organizations. A high proportion of the respondents confirmed the adequacy of implemented security controls to restrict physical access to their organizations' computer terminals, to the computer room, to hardware outside the computer room (such as network switch-gear, or modems) and to communications lines (for example, cables sealed in ducts outside the hardware area to prevent tapping or reading by service equipment) (Table III).

As Table III shows, 57.5 of the respondents indicated that their organizations' computer systems are located in areas physically isolated from the sprinkler system, to avoid water damage. Moreover, to avoid potential pollutants (such as smoke, dust, food and coffee) no smoking, eating or drinking is allowed around the computers in the majority of Saudi organizations. Slightly more than half of the respondents (53.5 percent) mentioned that waterproof covers are used in their organizations and merely half of the respondents believed that their organizations' computers are installed in secured areas, which are locked and kept under surveillance when not in use.

Table III also shows that a relatively high proportion of the respondents (61.1 percent) affirmed the adequacy of security controls implemented over generating and revoking the means of permitting physical access to their accounting systems (by keys, security badges, combination numbers, switch cards). Moreover, un-issued physical access media are reported to be under security control and all physical access procedures are subject to adequate supervision by a responsible person. Further, 58.5 percent of the respondents confirmed that the individuals who are responsible for controlling physical access are entirely independent of those who are responsible for the programming, system software, and accounting control functions in their organizations. Approximately 70 percent of the respondents confirmed that the above physical access procedures are subject to adequate supervision by a responsible official.

On the other hand, the majority of the respondents (76.5 percent) reported that their organizations' computers were not bolted to the desks and 64.4 percent of the total mentioned that no lockable covers are placed on the organizations' computers. However, many of them confirmed that they have disk-less computer machines. A high proportion of the respondents (almost 65 percent) confirmed the absence of internal trip alarms inside their computers. More than two-thirds of the respondents (almost 68.4 percent) revealed that neither alarms nor motion detectors are installed in areas with a high concentration of computer equipment in their organizations (Table III).

According to the statistics of the Kruskal-Wallis tests (Table XII), it seems that there are no significant differences among Saudi organizations regarding the existence and implementation of the hardware and physical access security controls at significance level p 0.05. Again, the Kruskal-Wallis test statistics (Table XIII) show no significant differences among the opinions of different respondent groups regarding the existence and implementation of the hardware and physical access security controls in their organizations at p 0.05.

Recommendation: Based on the previous empirical results, Saudi organizations are recommended to install alarms and motion detectors in areas with a high concentration of computer equipment. Installing computers only in areas that are locked and kept under surveillance when not in use, placing lockable covers on computers and bolting computer to desks or tables should be considered. Un-issued physical access badges and keys should be under adequate control and complete independence of individuals who are responsible for controlling physical access and those who are responsible for programming, system software, and accounting control functions should be considered.

5.3 Software and electronic access security controls

The statistical results in Table IV show that the majority of the organizations' respondents (82.9 percent) confirmed the installation of virus protection software in their accounting systems and that software is updated regularly. The vast majority of the respondents (86.2 percent) also confirmed that all the software used is original and that adequate procedures are in place to avoid the use of bootleg software and unauthorized copying of licensed software. Moreover, all backups and working copies of software and data are well maintained.

The vast majority of the respondents confirmed the existence of an adequate combination of software procedures and manual action to prevent unauthorized access and to report and investigate persistent attempts to bypass access controls. In addition, regular reports of unauthorized access are prepared and submitted to the organizations' management. A high proportion of the respondents (more than 82 percent) confirmed that strong password systems are used to identify individuals to the system as authorized

users. Adequate security procedures are implemented to ensure that the passwords are periodically changed, kept secret, and could not easily be guessed. Passwords are typically immediately cancelled for terminated or transferred organization employees.

From Table IV, it seems that there is adequate control over assigning access rights to appropriate individuals across Saudi organizations. Moreover, the majority of respondents confirmed the adequacy of the security controls implemented over granting and revoking authorized access on the system (such as user-IDs or passwords, access cards), allocating and withdrawing special facilities from users (for example, ability to use certain utilities, hierarchical levels of clearance) and protection of security tables stored on the system to verify authenticity (password control files, or communication control tables which can be one-way encrypted).

Moreover, most of the respondents (around 73 percent) reported that access security control functions (such as granting or changing system identities, granting or changing the ability to use special facilities, changing passwords, or other identification codes) are themselves restricted to appropriate organization staff, who have no incompatible duties. Furthermore, these procedures are subject to adequate supervision by a responsible official in the organization (Table IV). On the other hand, the vast majority of the respondents (85.1 percent) indicated that the current insurance covers neither software nor the cost of business interruption resulting from a computer mishap.

The results of the Kruskal-Wallis test (Table XII) show no significant differences among Saudi organizations regarding the existence of implementation of the software and electronic access security controls (at significance level p 0.05). On the other, the Kruskal-Wallis test (Table XIII) shows significant differences among the points of view of respondent groups regarding the existence and implementation of the software and electronic access security control counter-measures in their organizations (p 0.05).

Recommendation: Accordingly, it is advisable to extend current insurance to cover software and the cost of business interruption resulting from a computer mishap in Saudi organizations. Adequate procedures should be implemented to prevent unauthorized public access to the organizations' accounting information systems via dial-up (for example, by use of dial-back, and by dial-up access restricted to non-confidential information).

5.4 Data security controls

The results reveal that the great majority of the respondents (83.3 percent) affirmed the adequacy of security controls over the manual handling of input and output data in their organization (Table V). Moreover, 84.4 percent of respondents indicated that their organizations' data backups are routinely performed according to an appropriate schedule, at least daily for frequently updated data and monthly for infrequently changing data. Furthermore, all organization data backup media reportedly

have write protection in place. Again, the majority of the respondents confirmed that their organizations' data diskettes and cartridges are stored in a very strong, secure cabinet or a fire-rated safe. Additional backup copies of the organizations' data are usually kept in the nearest branch, for emergency and data recovery. According to 80 percent of the respondents a hard copy of particularly critical data is routinely made and securely stored. More than two-thirds of the respondents (68.4 percent) indicated that the backup schedules include hard disk backups as well.

Quite a high proportion of the respondents (67.3 percent) reported that unattended computers are turned off when data are removed from the system. Of the respondents, 64 percent confirmed that dealing with sensitive data is performed in private offices and only by designated officers to reduce the likelihood of their exposure (Table V). More than 75 percent of the respondents indicated the existence of documented emergency plans, which specified the main steps that should be taken when the systems failed, as well as the individuals who are responsible for completion of these steps.

On the other hand, a rather high proportion of the respondents (73.1 percent) reported that backups of sensitive data stored off-site are not encrypted to reduce the chance of unauthorized exposure. Moreover, around 58 percent of them indicated that data encryption has not been considered for sensitive data (such as the payroll, or organizations' customer lists). Approximately 63 percent of the respondents reported that legally binding confidentiality agreements are not drafted by employers and signed by employees who have access to sensitive data (e.g., customer lists). Moreover, 61 percent of the respondents confirmed that the format command is not left off the hard disk and reformatting of disks or overwriting of the files is not a requirement for extraction of sensitive data in their organizations. Finally, approximately 64 percent of them indicated that their organizations had not designated an adequate custodian for sensitive data disks (Table V).

The Kruskal-Wallis test statistics show no significant differences among different organizations (Table XII) and respondent group views (Table XIII) regarding the existence and implementation of data security controls counter-measures in the Saudi environment (at p 0.05).

Recommendation: According to the above results, it is recommended that sensitive data stored off-site should be encrypted to reduce the chance of its unauthorized exposure, legally binding confidentiality agreements related to sensitive data should be enhanced and adequate provision for the custody of sensitive data disks and backups should be strengthened in Saudi organizations.

5.5 Off-line programs and data security controls

Off-line computer software and backup copies of data and programs in the physical library are no less important than the working data and programs. The questionnaire data (Table VI) revealed that the majority of respondents (82.2 percent) confirmed the existence of adequate records to identify off-line programs and data stored in unique media, where each individual item has external labels for easy recognition.

The findings also show that the majority of the respondents (76.4 percent) confirmed the adequacy of security controls over the issuing and returning of programs or data files to and from a physical computer library, either for installation or for disaster recovery. Furthermore, of the respondents, 78.9 percent indicated that the storage methods in their organizations to prevent unauthorized removal of stored data and programs are adequate and all the previous procedures are subject to adequate supervision by a responsible official in the organization (Table VI). On the other hand, more than two thirds of the respondents (68.7 percent) mentioned that the librarian functions in their organizations are not performed by individuals entirely independently of computer operation and programming responsibilities.

The Kruskal-Wallis test (Table XII) provides strong evidence that there are no significant differences among different Saudi organizations. In contrast, the Kruskal-Wallis test (Table XIII) shows significant differences among respondent groups regarding their opinions on the existence and implementation of off-line program and data security control counter-measures in Saudi organizations (at p 0.05).

Recommendation: It can be concluded that better security controls should be implemented over the issuing and returning of program/data files to and from physical libraries. Moreover, the librarian functions should be performed by individuals who are entirely independent of computer operation and programming responsibilities.

5.6 Utility security controls

The results reveal that around two thirds of the respondents (66.3 percent) confirmed the adequacy of control procedures implemented to identify all utility programs and other special programs (which could be used, for example, to change application programs or data, by bypassing normal software access restrictions in their organizations). Approximately 55 percent of respondents agreed that the ability to use such programs is restricted to appropriate and authorized individuals in their organizations (Table VII). Moreover, 57.5 percent of the respondents confirmed the adequacy of implemented controls to log and report the use – or even attempt at use – of such programs. Furthermore, a regular review of such reports is reported to be carried out, usually by a responsible official in the organization, to determine and investigate any unauthorized access to the organization's CAIS.

According to the Kruskal-Wallis test (Table XII) it seems that there are no significant differences among different organizations (at p 0.05) regarding the existence

and implementation of the utilities security control in Saudi organizations. On the other hand, the Kruskal-Wallis test (Table XIII) shows significant differences among the opinions of different respondent groups regarding the existence and implementation of the utilities security control countermeasures in Saudi organizations (again, at significance level p 0.05).

Recommendation: Based on the above results, more attention should be directed by Saudi organizations to strengthen utility security controls, to identify all utility programs or other special programs and to implement adequate security controls over the use, or even attempts at use, of such programs.

5.7 Bypassing of normal access security controls

Sometimes it becomes a necessity to bypass normal security controls, to achieve specific authorized tasks by internal or external individuals (emergencies, or maintenance of program libraries by outside software support, such as software vendors, through dial up). In these cases, it is very important to keep such actions under strong restrictive security control. The results reveal that 63.3 percent of the organizations' respondents confirmed the existence of appropriate authorization procedures and adequate security controls for bypassing normal security controls (Table VIII). Approximately 61 percent of the respondents agreed on the adequacy of implemented security controls to prevent, investigate and report any unauthorized changes to their organizations' data files. Moreover, adequate security controls are in place to ensure that security is subsequently reinstated whenever normal security controls are bypassed in cases of emergency.

The Kruskal-Wallis test (Table XII) provides strong evidence that there are significant differences among Saudi organizations (at p 0.05), while no significant differences appear among different respondent groups (Table XIII) regarding the existence and implementation of the bypassing of normal access security controls in the Saudi environment (at significance level p 0.05).

Recommendation: Stronger security should be implemented regarding the bypassing of normal access controls to prevent, investigate and report any unauthorized changes to organizations' data files. Furthermore, adequate controls should be in place to ensure that security is subsequently reinstated whenever bypassing of normal security controls has occurred in emergency cases.

5.8 User programming security controls

High level programming languages could be used to change organizations' data and manipulate programs and files. The results (Table IX) reveal that slightly more than half of respondents (56.4 percent) agreed on the existence and implementation of adequate security controls over the use of such programs. They confirmed the existence of appropriate security controls to prevent unauthorized use of high level programming

languages, or even an attempt to use them. However, almost half of the respondents (48.4 percent) agreed that their organizations did not have adequate security controls in place to prevent and report unauthorized use of programs written by unauthorized users.

The Kruskal-Wallis test provides strong evidence that there is a significant difference among both organization types (Table XII) and respondent groups (Table XIII) regarding the existence and adequacy of implemented user programming security controls in Saudi organizations (at p 0.05).

Recommendation: The results suggest that there is a need to implement stronger security controls to prevent the unauthorized use of high level programming languages. Adequate security controls should be implemented to prevent and report unauthorized use of programs written by unauthorized users in Saudi organizations.

5.9 Division of duties

A high proportion of the respondents (70 percent) confirmed the segregation of incompatible accounting duties and tasks in their organizations (that is authorization, record keeping and custody). However, a similar segregation is also required regarding incompatible computer tasks, to reduce the likelihood of breaching CAIS security controls. A majority of the respondents (80.4 percent) agreed on the adequacy of the implementation of security controls to prevent computer operators, schedulers, data input staff, and other operations personnel from gaining access to program documentation and development libraries in their organizations.

Almost 63 percent of the respondents indicated that computer programmers and development personnel are not allowed to gain access to the computer operations areas in their organizations. Further, 50.2 percent of the respondents agreed on the adequacy of the implemented security controls to prevent systems personnel who are responsible for cataloguing functions from gaining access to program documentation and development libraries and to prevent them from entering the operations area or performing computer operations functions in their organizations (Table X).

The Kruskal-Wallis test (Table XII) displays significant differences among different organizations regarding the existence and implementation of division of duties in Saudi organizations. However, it seems that there are no significant differences in the opinions of respondent groups (Table XIII) regarding the adequacy of the implemented security controls to prevent computer operators, schedulers, data input staff, and other operations personnel from gaining access to program documentation and development libraries in their organizations (at p 0.05).

Recommendation: In the light of the above, it is suggested that Saudi organizations should pay more attention to the segregation of incompatible computer

tasks and duties. A clear and strict procedure should be put in place to prevent computer operators, schedulers, data input staff, and other operations personnel from gaining access to program documentation and development libraries. Moreover, systems personnel who are responsible for cataloging functions should be prevented from gaining access to program documentation and development libraries, as well as preventing them from entering the operations area or performing computer operations functions.

5.10 Output security controls

The majority of the respondents (77.1 percent) confirmed that all sensitive data in their organization are secure and protected. Visual access to the organizations' sensitive information is strongly controlled and restricted only to authorized users at the authorized time. Almost 71 percent of the respondents indicated that their organizations' sensitive computer output is secured in a locked cabinet, and that strong security procedures are implemented whenever some of these sensitive data are printed outside the data centre or central computer room. According to the majority of respondents (72.7 percent), shredding machines are available and used in their organizations for disposal of confidential and sensitive data. Moreover, this task is restricted to security-cleared individuals in the organization (Table XI).

The vast majority of the respondents (almost 95 percent) confirmed that input to output reconciliation is adequately implemented in their organizations. A very high proportion of the respondents (87.6 percent) reported that all their organizations' hard copy documents and output are automatically date and time-stamped. Moreover, 78.2 percent of the respondents confirmed the adequacy of the implemented security controls over printing, copying and distributing of their computer output and reports. Further, all the previous tasks are restricted to the authorized individuals in the organization. In addition, random output/input comparisons are regularly carried out to verify correct processing.

The Kruskal-Wallis test (Table XII) provides strong evidence that there are significant differences among organizations regarding the adequacy of implemented output security controls in Saudi organizations (at significance level p 0.05). Furthermore, it seems that there are significant differences among respondent groups (Table XIII) regarding the existence and implementation of the output security control counter-measures in their organizations (again at p 0.05).

Recommendation: According to the above results, it seems that, while the majority of the respondents in the Saudi organizations confirmed the adequacy of implemented security controls over printing, copying and distributing its output, more adequate output security controls should be put in place and directed to secure and protect sensitive organization data across Saudi organizations.

6. Conclusion

In this paper an empirical survey was carried out to investigate the existence and adequacy of implemented CAIS security controls in Saudi organizations. The paper also investigates the significant differences among different Saudi organizations as well as among respondent groups regarding the above research issues. The statistical results highlighted a number of inadequately implemented CAIS security controls in Saudi organizations and accordingly, some suggestions to eliminate these weak points are recommended.

According to the survey results, it is recommended to restrict access to organizations' sensitive data to the authorized employees with defined needs. Mandatory vacations of employees should be considered and enhanced personnel policies, including the rotation of duties should be enhanced. It is recommended that alarms and motion detectors should be installed in areas with a high concentration of computer equipment. Installing computers only in areas that are locked and kept under surveillance when not in use, placing lockable covers on computers and bolting computer to desks or tables should be considered. Further, un-issued physical access badges and keys should be under adequate control. Restrictions on the complete independence of individuals who are responsible for controlling physical access and those who are responsible for programming, system software, and accounting control functions should also be considered.

Adequate procedures should be implemented to prevent unauthorized access CAIS. Moreover, sensitive data stored off-site should be encrypted to reduce the chance of its unauthorized exposure; legally binding confidentiality agreements related to sensitive data should be enhanced and adequate custody of sensitive data disks and backups should be strengthened in Saudi organizations.

Adequate security controls should be implemented over the issuing and returning of program/data files to and from physical libraries. Librarian functions should be performed by individuals who are entirely independent of computer operation and programming responsibilities. More attention should be directed by Saudi organizations to strengthen utility security controls, to identify all utility programs or other special programs and to implement adequate security controls over the use, or even attempted use, of such programs. Stronger security should be implemented in the bypassing of normal access controls to prevent, investigate and report any unauthorized changes to organizations' data files. Furthermore, adequate controls should be in place to ensure that security is subsequently reinstated whenever bypassing of normal security controls has occurred in emergency cases.

Segregation of incompatible computer tasks and duties should be considered. A clear and strict procedure should be put in place to prevent computer operators, schedulers, data input staff, and other operations personnel from gaining access to program documentation and development libraries. Moreover, systems personnel who are responsible for cataloging functions should be prevented from gaining access to program documentation and development libraries, as well as preventing them from entering the operations area or performing computer operations functions. Moreover, adequate output security controls should be put in place and directed to secure and protect sensitive data across Saudi organizations.

Further investigation could be undertaken to extend and improve this research. The intention of the current research has been to evaluate the security controls of CAIS in Saudi organizations. However, more research is needed to obtain evidence from other developing countries in the Middle East and Gulf countries. Comparative studies could be carried out to investigate the significant differences between developing and developed countries regarding the adequacy and effectiveness of implemented CAIS security controls. Investigating the differences in the opinions of CAIS programmers and designers, internal auditors, external auditors and CAIS operational staff could be potential avenues for future research.

References

[1] Abu-Musa, A. A. (2004a), "The Threats of Computerized Accounting Information Systems: An Empirical Study on Saudi Organizations", *The Public Administration Journal*, The Public Administration Institute, Riyadh, Saudi Arabia, Vol. 44, No. 3, pp. 509 – 570.

[2] Abu-Musa, A. A. (2004b), "Investigating The Security Policies of Computerized Accounting Information Systems in the Banking Industry of an Emerging Economy: The Case of Egypt", *The Business Review of Information Systems*, USA, Summer. Vol. 8, Number 3, pp. 83 -102.

[3] Abu-Musa, A. A. (2004c), "Investigating the Security Controls of CAIS in an Emerging Economy: An Empirical Study on Egyptian Banking Industry", *The Journal of Managerial Auditing, UK*, Vol. 19, Iss.2, pp. 272 -302.

[4] Abu-Musa, A. A. (2002), "Computer Crimes: How Can You Protect Your Computerized Accounting Information System", *The Journal of American Academy of Business, Cambridge, USA*, Vol. 2. No.1 September 2002, pp. 91-11.

[5] Al-Sudairy M. A., and N. K. Tang (2000), "Information Technology in Saudi Arabia's Supermarket Chains", *International Journal of Retail & Distribution Management*, Vol. 28 No.8, pp. 341-356.

[6] Boockholdt, J. L. (1989), "Implementing Security and Integrity in Macro-Mainframe Networks", *MIS Quarterly*, (June), PP.135 -144.

[7] Buttross, T. E. and M. D. Ackers (1990), "A Time - Saving Approach To Microcomputer Security", *Journal Of Accounting & EDP,* (Vol. 6, Iss. 1), pp. 31 - 35.

[8] 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.

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

[10] Committee of Sponsoring Organizations of the Treadway Commission (COSO). 1992. Internal Control: Integrated Framework (COSO, New York).

[11] Crockett, B. (1993), "Banks Are Leaders in Computer Security", *American Banker*, (Nov.), p. 20.

[12] Curtiss, R.H. (1995), "Four years after massive war expenses Saudi Arabia get its second wind," *The Washing ton Re port on Middle East Affairs*, (September), pp.48- 52.

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

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

[15] Dhillon, G. and J. Backhouse (2000), "Information Systems Security Management in the New Millennium", *Association for Computing Machinery, Communication of the ACM,* New York, (Vol. 43, Iss. 7), PP. 125-129.

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

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

[18] Furnell, S. M., P. S. Dowland (2000), "A conceptual architecture for real-time intrusion monitoring", *Information Management & Computer Security*, (Vol. 8, Iss. 2), PP.65-75.

[19] Henry, L.; (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.

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

[21] Hood, K. 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.

[22] Hunton, J.; A. Wright; and S. Wright, (2004), "Are financial auditors overconfident in their ability to assess risks associated with enterprise resource planning systems? *Journal of Information Systems*, (Vol. 18, No. 2), PP. 7-28.

[23] Information Security Management, Part2: Specification for Information security management systems AS/NZS 7799.2:2003, BS 7799.2:2002

[24] Information Technology – Code of practice for Information Security Management AS/NZS ISO/IEC 17799:2001
[25] Information Systems Audit and Control Foundation (ISACF); (1998); *Control Objectives for Information and Related Technology (COBIT)*; (ISACF, Rolling Meadows, Il).
[26] International Federation of Accountants (IFAC), Information Technology Committee, (1998), *International Information Technology Guidelines: Managing Security of Information,* (January), New York.
[27] Jasimuddin, S. (2001), "Analyzing the competitive advantages of Saudi Arabia with Porter's model", *Journal of Business and Industrial Marketing*, Vol. 16 No.1, pp.59-68.
[28] Jenkins, B.; P. Cooke; and P. Quest (1992), *An Audit Approach to Computers,* (Institute of Chartered Accountants in England and Wales, Moorage Place, London).
[29] KPMG (2000), *Information Security Survey 2000, Executive Summary*, April, KPMG, London.
[30] Mau, S.; and J. Catlin (1993), "Systems Security In 90's", *Interpreter*, (January), pp. 8-9.
[31] Meall, L. (1992), "Computer Crime: Foiling the Fraudsters", *Accountancy,* (November), pp. 56-57.
[32] Melville S and W. Goddard (1996) *Research Methodology: An Introduction for Science and Engineering Students*, Juta and Co. Ltd, Kenwyn.
[33] Miller, D. C. (1991) *Handbook of Research Design and Social Measurement,* (Fifth Edition), SAGE Publications, London.
[34] National Institute of Standards and Technology (1996), Technology Administration, U.S. Department of Commerce, *Generally Accepted Principles and Practices for Securing Information Technology Systems*, September.
[35] National Institute of Standards and Technology (1998), Federal Computer Security Program, Managers' Forum Working Group, *Guide for Developing Security Plans for Information Technology Systems,* Special Publication 800-18, December.
[36] 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.
[37] Public Oversight Board (POB). 2000. The Panel on Audit Effectiveness: Report and Recommendations, 2000, www.pobauditpanel.org.
[37] 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.
[38] Rockwell, R. (1990), "The Advent of Computer Related Crimes", *Secured Lender*, (Jul /Aug), pp. 40 - 42
[39] Sohail M., and O. Al-Abdali (2005), "The usage of third party logistics in Saudi Arabia Current position and future prospects", *International Journal of Physical Distribution & Logistics Management*, Vol. 35 No. 9, pp. 637-653.
[40] Solms, Rossouw Von (1996), "Information Security Management: The Second Generation", *Computer & Security (UK)*, pp. 281 - 288.
[41] 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.
[42] The United States General Accounting Office (GAO) (2003), *Information Security: Computer Controls over Key Treasury Internet Payment System*, Report to Congressional Requesters, July.
[43] Wackerly, D. D., W. Mendenhall and R. L. Scheaffer (1996) *Mathematical Statistics with Applications,* Duxbury Press, Wadsworth Publishing Company, London.
[44] Warren, M. J. (2002), Security practice: survey evidence from three countries, *Logistics Information Manageme,* (Vol. 15, Iss. 5/6), PP. 347-351.
[45] White, G. W. and S. J Pearson (2001) "Controlling corporate e-mail, PC use and computer security"; *Information Management & Computer Security*, Vol. 9, Iss. 2/3; pp. 88-93.
[46] 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.

[47] Yavas, U. and M. Yasin (1994), Manufacturing versus Service Organizations: An Investigation of Informational and Operational Interactions in the International Domain" *Industrial Management & Data Systems*, Vol. 94, No. 4, pp. 24-29.

[48] Yavas, U. (1997), "Management Know-How Transfer To Saudi Arabia: A Survey of Saudi Managers", *Industrial Management & Data Systems*, Vol. 97, No. 7, pp. 280-286.

[49] Yavas, U. and M. Yasin (1999) "Organizational Significance and Application of Computer Skills: A Culturally- Based Empirical Examination", *Cross cultural Management – An International Journal,* Volume 6 Number 4.

[50] Zviran, M., and W. J. Haga, (1999), "Password Security: An Empirical Study", *Journal of Management Information Systems*, Vol.15, Iss.4; pp. 161-185.

Appendixes

Table I. The research sample

The Research Sample According to Business Type			The Research Sample According to Respondents Type		
Type of Business	Frequency	Percent	Job Title	Frequency	Percent
Manufacturing	61	22.2	Internal Auditor	39	14.2
Banking	34	12.4	Staff Accountant	99	36.0
Insurance	20	7.3	Cost Accountant	20	7.3
Retail Merchandising	41	14.9	Controller	36	13.1
Services	22	8.0	EDP Auditor	4	1.5
Government	25	9.1	Manager	55	20.0
Oil	17	6.2	Other	22	8.0
Health Care	18	6.5			
Other	37	13.5			
Total	275	100.0	Total	275	100.0

Table II. Organizational security controls

Organizational Security Controls	**Exist**		**Do Not Exist**	
	Frequency	**Percent**	**Frequency**	**Percent**
1- Management attitude toward the security of the computerized accounting information system as reflected by its actions is appropriate.	**205**	**74.5**	**70**	**25.5**
2- Rotation of duties is utilized to increase the chance of exposure of errors and irregularities.	**174**	**63.3**	**101**	**36.7**
3- Mandatory vacations used to reduce the likelihood of fraud or embezzlement resulting from increased chance of exposure.	**125**	**45.5**	**150**	**54.5**
4- Personnel policies include background checks to reduce the likelihood of hiring dishonest employees.	**202**	**73.5**	**73**	**26.5**
5- There is documentation showing that users have been properly trained.	**151**	**54.9**	**124**	**45.1**
6- The employees who have access to sensitive data have been bonded.	**94**	**34.2**	**181**	**65.8**

Table III. Hardware and physical access security controls

Hardware and Physical Access Security Controls	Exist		Do Not Exist	
	Frequency	Percent	Frequency	Percent
1- Adequate theft and hazard insurance covering computers' hardware.	**227**	**82.5**	**48**	**17.5**
2- Limiting computer access to employees with a defined need.	**214**	**77.8**	**61**	**22.2**
3- Installing computers only in areas that are locked and kept under surveillance when not in use.	**140**	**50.9**	**135**	**49.1**
4- Bolting computer to desks or tables.	**65**	**23.6**	**210**	**76.5**
5- Placing lockable covers on computers.	**98**	**35.6**	**177**	**64.4**
6-Installing alarms and motion detectors in areas with high concentration of computer equipment.	**100**	**36.4**	**175**	**64.6**
7- Placing internal trip alarms inside computers.	**87**	**31.6**	**188**	**68.4**
8- Line co-coordinators to smooth out power.	**228**	**82.9**	**47**	**17.1**
9- Un-interruptible power supply units to supply power during power outages.	**231**	**84**	**44**	**16**
10- Extinguishers exist and close at hand.	**217**	**78.9**	**58**	**21.2**
11- Placement of computers away from the sprinkler system to avoid water damage.	**158**	**57.5**	**117**	**42.5**
12- Waterproof covers to avoid water damage	**147**	**53.5**	**128**	**46.5**
13- Implementation of a smoking ban, or use of small fans around the computer to blow any smoke away from the system.	**172**	**62.5**	**103**	**37.5**
14- Avoidance of other potential pollutants (e.g., dust, food, and coffee) around the computer.	**197**	**71.6**	**78**	**28.4**
15- There are adequate controls to restrict physical access to the following:				
A. terminals,	**202**	**73.5**	**73**	**26.5**
B. computer room,	**211**	**76.7**	**64**	**32.3**
C. hardware outside the computer room (e.g. network switch-gear, modems),	**182**	**66.2**	**93**	**33.8**
E. communications lines (e.g., cables should be sealed in ducts outside the hardware area to prevent tapping or reading by service equipment).	**191**	**69.5**	**84**	**30.5**
16- Adequate controls over:				
A. generating and revoking the means of permitting physical access (e.g. key, security badge, combination number, switch card);	**168**	**61.1**	**107**	**38.8**
B. where applicable, un-issued physical accesses permit badges or keys?	**146**	**53.1**	**129**	**46.9**
17- The person responsible for controlling physical access should be independent of programming, system software, and accounting control functions.	**161**	**58.5**	**114**	**41.5**
18- The previous physical access procedures are subject to adequate supervision by a responsible official.	**192**	**69.8**	**83**	**30.2**

Table IV. Software security & access security controls

Software Security and Access Security Controls	Exist		Do Not Exist	
	Frequency	Percent	Frequency	Percent
1- Virus protection software should be installed.	**228**	**82.9**	**47**	**17.1**
2- Sensitive data transmitted should be encrypted.	**151**	**54.9**	**124**	**45.1**
3- The present insurance should cover software.	**119**	**43.3**	**156**	**56.7**
4- Insurance extended to cover the cost of business interruption resulting from a computer mishap.	**41**	**14.9**	**234**	**85.1**
5- Backups and working copies of software and data are well maintained.	**243**	**88.4**	**32**	**11.6**
6- Software backups, like originals, should have write-protect tabs in place.	**237**	**86.2**	**38**	**13.8**
7- Originals placed in an off –site storage (e.g., a safe-deposit box or the home of the owner or chief executive officer).	**163**	**59.3**	**112**	**40.7**
8- Adequate steps should be taken to avoid unauthorized copying of licensed software.	**209**	**76**	**66**	**24**
9- Adequate steps should be taken to avoid the use of bootleg software.	**218**	**79.3**	**57**	**20.7**
10- There is an adequate combination of software procedures and manual action to:				
A. prevent unauthorized accesses, report and investigate persistent attempts to bypass the access controls, or	**230**	**83.6**	**45**	**16.4**
B. report and investigate unauthorized accesses.	**233**	**84.7**	**42**	**15.3**
11- Are there controls over:				
A. assigning access rights to appropriate individual in the organization,	**206**	**74.9**	**69**	**25.1**
B. granting and revoking authorized access on the system (e.g., user -IDs or passwords, switch cards, visa cards),	**204**	**74.2**	**71**	**25.8**
C. allocating and withdrawing special facilities from users (e.g., ability to use certain utilities, higher levels of clearance in a hierarchy),	**195**	**70.9**	**80**	**29.1**
D. protecting the security tables stored on the system, which are used by the system to verify authenticity (e.g., password control files, communication control tables can be one-way encrypted).	**197**	**71.6**	**78**	**28.4**
12. Passwords (or other codes) are used to identify individuals to the system as authorized users; are there adequate procedures to ensure that the passwords are:				
A. periodically changed,	**226**	**82.2**	**49**	**17.8**
B. kept secret (e.g., not written down or displayed on screen),	**231**	**84.0**	**44**	**16.0**
C. not easily guessed, and	**227**	**82.5**	**48**	**17.5**
D. cancelled for terminated or transferred employees.	**227**	**82.5**	**48**	**17.5**

Software Security and Access Security Controls	Exist		Do Not Exist	
	Frequency	Percent	Frequency	Percent
13- Adequate procedures should be implemented to ensure the ability to use the following access control functions are itself restricted to appropriate staff with no other incompatible duties:				
A. granting or changing systems identities,	**199**	**72.4**	**76**	**27.6**
B. granting or changing the ability to use special facilities,	**210**	**76.4**	**65**	**23.6**
C. changing passwords or other identification codes.	**194**	**70.5**	**81**	**29.5**
14- Adequate procedures should be implemented to prevent unauthorized public access via dial-up (e.g. use dial-back, dial-up access restricted to non-confidential information).	**159**	**57.8**	**116**	**42.2**
15-All the above procedures should be subject to adequate supervision by a responsible organization's official.	**203**	**73.8**	**72**	**26.2**

Table V. Data security controls

Data Security Controls	Exist		Do Not Exist	
	Frequency	Percent	Frequency	Percent
1- Security controls implemented over manual handling of input and output data among the organization's departments are adequate:	**229**	**83.3**	**46**	**16.7**
2- Data backups should be routinely prepared.	**232**	**84.4**	**43**	**15.6**
3- Backups are being performed on schedule where:				
A. at least daily for frequently updated data,	**232**	**84.4**	**43**	**15.6**
B. at least monthly for data that changes infrequently.	**241**	**87.6**	**34**	**12.4**
4- Data backups should have write-protect tabs in place.	**203**	**73.8**	**72**	**26.2**
5- A copy of backups should be placed in an off-site storage.	**148**	**53.8**	**127**	**46.2**
6- Backups of sensitive data that are stored off-site should be encrypted to reduce the chance of unauthorized exposure.	**74**	**26.9**	**201**	**73.1**
7- A hard copy should be routinely printed for particularly critical data.	**220**	**80.0**	**55**	**20.0**
8- Hard disks include an external hard disk or cassette tape as a backup	**188**	**68.4**	**87**	**31.6**
9- The FORMAT command should be left off the hard disk	**107**	**38.9**	**168**	**61.1**
10- Data encryption should be considered for sensitive data (e.g., payroll).	**116**	**42.2**	**159**	**57.8**
11- Work on sensitive data should be limited to private offices to reduce the likelihood of exposure.	**176**	**64.0**	**99**	**36.0**
12- The organization should have designated	**100**	**36.4**	**175**	**63.6**

Data Security Controls	Exist		Do Not Exist	
	Frequency	Percent	Frequency	Percent
adequate custody for sensitive data disks.				
13-Unattended computers should be turned off when data is removed from the system.	**185**	**67.3**	**90**	**32.7**
14- Reformatting of the disk or overwriting of the file should be required for extraction of sensitive data.	**122**	**44.4**	**153**	**55.6**
15-Legally binding confidentiality agreements should be drafted by employers and signed by computer users with access to sensitive data (e.g., customer lists).	**102**	**37.1**	**173**	**62.9**
16- Diskettes or cartridges should be stored in a secure cabinet or fire-rated safe.	**270**	**98.2**	**5**	**1.8**
17- A documented emergency plan should state:				

Table VI. Off-line programs and data security controls

Off-line Programs and Data Security Controls	Exist		Not Exist	
	Frequency	Percent	Frequency	Percent
1- Where programs and data, including back-up copies, are physically controlled:				
A. Adequate records should be kept to identify programs/ data uniquely (e.g. external labels)	**226**	**82.2**	**49**	**17.8**
B. Adequate security controls should be implemented over issuing and returning of programs/data files:				
• to and from the physical library,	**210**	**76.4**	**65**	**23.6**
• to and from the store to be used for recovery in the event of a disaster,	**210**	**76.4**	**65**	**23.6**
• to and from the installation ,	**210**	**76.4**	**65**	**23.6**
C. Storage methods should prevent the unauthorized removal of programs/data	**217**	**78.9**	**58**	**21.1**
2- The librarian function should be performed by a person independent of computer operation and programming responsibilities	**86**	**31.3**	**189**	**68.7**
3- The above procedures should be subject to adequate supervision by a responsible official	**217**	**78.9**	**58**	**21.1**

Table VII. Utility security controls

Utility Security Controls	Exist		Not Exist	
	Frequency	Percent	Frequency	Percent
1-If utilities or other special programs could be used to change application programs/ data by bypassing normal software access restrictions:				
A. Adequate procedures should be implemented to identify all programs with this special status,	**182**	**66.2**	**93**	**33.8**
B. The ability to use such programs should be restricted to appropriate , authorized personnel in the organizations	**151**	**54.9**	**124**	**45.1**
C. Adequate security controls to log and report				

Utility Security Controls	Exist		Not Exist	
	Frequency	Percent	Frequency	Percent
the use, or attempted use, of such programs should be implemented. A review of such reports should be performed by a responsible official to determine and investigate unauthorized access.	**158**	**57.5**	**117**	**42.5**

Table VIII. Bypassing of normal access security controls

Bypassing of Normal Access Security Controls	Exist		Not Exist	
	Frequency	Percent	Frequency	Percent
1- Where it is necessary to bypass normal security controls (e.g. emergencies or maintenance of program libraries by outside software support, such as vendor, through dial up):				
A. is there appropriate authorization before or after the event,	**174**	**63.3**	**101**	**36.7**
B. are there adequate controls to :				
1-ensure that security is subsequently reinstated,	**167**	**60.7**	**108**	**39.3**
2-prevent or report and investigate unauthorized changes to data?	**160**	**58.2**	**115**	**41.8**

Table IX. User programming security controls

User Programming Security Controls	Exist		Not Exist	
	Frequency	Percent	Frequency	Percent
1- Where users are permitted to use utilities or high level programming languages which can change data:-				
A- Adequate security controls should be implemented to prevent the unauthorized use of this facility, and to report and investigate unauthorized use or attempts to use it,	**155**	**56.4**	**120**	**43.6**
B- - Adequate security controls should be implemented to prevent and report unauthorized use of programs written by unauthorized user.	**142**	**51.6**	**133**	**48.4**

Table X. Division of duties security controls

Division of Duties	Exist		Not Exist	
	Frequency	Percent	Frequency	Percent
1- Is a segregation of accounting duties (i.e., authorization, record keeping, and custody) good and adequate?	**191**	**69.5**	**84**	**30.5**
2- Are there adequate controls to prevent:				
A. Computer operators, schedulers, data input staff, and other operations personnel from	**221**	**80.4**	**54**	**19.6**

Division of Duties	Exist		Not Exist	
	Frequency	Percent	Frequency	Percent
gaining access to program documentation and development libraries,				
B. Development personnel from gaining access to the computer operations area,	**172**	**62.5**	**103**	**37.5**
C. Systems implementation personnel responsible for cataloguing function from gaining access to program documentation and development libraries, and from entering the operations area or performing computer operations functions?	**138**	**50.2**	**137**	**49.8**

Table XI. Output security controls

Output Security Controls	Exist		Not Exist	
	Frequency	Percent	Frequency	Percent
1. Visual access to sensitive information should be controlled and restricted only to the authorized users in the authorized time.	**212**	**77.1**	**63**	**22.9**
2. Printing of sensitive data outside the data centre or central computer room should be under security controls	**195**	**70.9**	**80**	**29.1**
3. Sensitive computer output should be secured in a locked cabinet	**206**	**74.9**	**69**	**25.1**
4. Hard copy output should be automatically date/time stamped.	**241**	**87.6**	**34**	**12.4**
5. Adequate controls should be implemented over the distribution of computer output and reports	**215**	**78.2**	**60**	**21.8**
6. Copying of computer output should be restricted to authorized individuals in the organization	**218**	**79.3**	**57**	**20.7**
7. Adequate security controls should be implemented over printed copies of data / information	**206**	**74.9**	**69**	**25.1**
8. Printing and distribution of data and information done should be under proper security controls, and only by authorized persons in the organization.	**182**	**66.2**	**93**	**33.8**
9. Shredding machines should be available and used for disposal of confidential data	**225**	**81.8**	**50**	**18.2**
10. Shredding of sensitive documents should be restricted to security cleared personnel.	**200**	**72.7**	**75**	**27.3**
11. Input to output reconciliation should be implemented.	**261**	**94.9**	**14**	**5.1**
12. Random output / input comparisons should be regularly done to verify correct processing.	**239**	**86.9**	**36**	**13.1**

Table XII. The Results of kruskal wallis test according to business type

	Organizational Security Controls	Hardware Security Controls	Software Security Controls	Data Security Controls	Off-line Data & Program Security Controls
Chi-Square	22.498	14.581	14.649	12.474	13.109
df	8	8	8	8	8
Asymp. Sig.	.004	.068	.066	.131	.108

	Utility Security Controls	Bypassing Security Controls	User Programming Security Controls	Division of Duties	Output Security Controls
Chi-Square	12.386	15.700	26.644	31.156	29.403
df	8	8	8	8	8
Asymp. Sig.	.135	.047	.001	.000	.000

Table XIII. The Results of Kruskal Wallis test according to respondents type

	Organizational Security Controls	Hardware Security Controls	Software Security Controls	Data Security Controls	Off-line Data & Program Security Controls
Chi-Square	4.401	9.366	21.103	7.057	21.235
df	6	6	6	6	6
Asymp. Sig.	.623	.154	.002	.316	.002

	Utility Security Controls	Bypassing Security Controls	User Programming Security Controls	Division of Duties	Output Security Controls
Chi-Square	13.848	8.322	31.121	9.065	17.073
df	6	6	6	6	6
Asymp. Sig.	.031	.215	.000	.170	.009

تقييم الضوابط الرقابية لأمن نظم المعلومات المحاسبية الإلكترونية في المنشأت السعودية: دراسة ميدانية

أحمد عبد السلام أبو موسى

قسم المحاسبة ونظم المعلومات الإدارية

جامعة الملك فهد للبترول والمعادن، الظهران، المملكة العربية السعودية

(قدّم للنشر في ٢٠٠٥/١٠/٠٨م؛ وقبل للنشر في ٢٠٠٦/٠٤/٠٨م)

ملخص البحث . يهدف هذا البحث إلى تقييم وجود ومدى كفاية الضوابط الرقابية المطبقة لحماية 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 تم توزيع عدد خمسمائة قائمة إستقصاء على عينة عشوائية من المنشأت السعودية، حيث تم تجميع وتحليل عدد مائتين وخمس وسبعين قائمة إستقصاء مكتملة وصالحة لأغراض التحليل. ولقد أظهرت نتائج الدراسة عدداً من نواحى القصور وعدم كفاية الضوابط الرقابية المطبقة فى تلك المنشأت والمتعلقة بحماية أمن نظم المعلومات المحاسبية الإلكترونية ضد المخاطر المختلفة التى تهدد أمن تلك النظم. ولقد قدمت الدراسة عدداً من المقترحات والتوصيات التى يمكن أن تسهم فى تدعيم وتعزيز الضوابط الرقابية الخاصة بأمن نظم المعلومات المحاسبية الإلكترونية في المنشأت السعودية. ومن الناحية العملية فإن نتائج هذه الدراسة سوف تمكن مديرى المنشأت والمراجعين الداخليين والخرجيين وغيرهم من المهنيين ومستخدمى نظم المعلومات المحاسبية الإلكترونية من فهم وتقييم حالة أمن نظم المعلومات المحاسبية الإلكترونية في المنشأت السعودية والتعرف على نواحى القصور بها، ومن ثم إمكانية إتخاذ القررات التصحيحية المناسبة

لتلافى أوجه القصور المختلفة، وتعزيز الضوابط الرقابية الأمنية لتلك النظم بما يحقق الإستفادة المثلى من تكنولوجيا المعلومات في المنشأت السعودية.