Investigating The Security Policies Of Computerized Accounting Information Systems In The Banking Industry Of An Emerging Economy: The Case Of Egypt

Dr. Ahmad A. Abu-Musa, Tanta University, Egypt

Abstract

Information has become one of the most valuable corporate assets, which should be protected with care and concern because business survival and success are heavily dependent upon the confidentiality, integrity and continued availability of critical information. The reliance on information and rapidly changing technology forces many organizations to implement comprehensive information security programs to protect their information systems. However, the success of implementing such security programs relies largely on employees' awareness and compliance. The failure to secure information or to make it available when required to those who need it would lead to financial and non-financial losses. The objective of this paper is to explore the main characteristics of security policies of the computerised accounting information systems (CAIS) in the Egyptian Banking Industry (EBI), and to investigate the differences among bank types regarding the existence, implementation, clarity, comprehensiveness, publicity, awareness, management attitudes, and participation in designing, developing and evaluating their banks' CAIS security policies. The research statistics revealed that the vast majority the surveyed banks has formal written, clear, comprehensive, reasonable and well-published CAIS security policies. Moreover, the majority of respondents believed that there was adequate awareness of CAIS security issues among their banks' managers and employees and that managers had positive attitudes and paid great attention to security issues. Further, the majority of respondents also claimed that they participated in designing, developing and evaluating their banking CAIS security policies and controls.

Introduction

Information has become one of the most valuable corporate assets, which should be protected with care and concern because business survival and success are heavily dependent upon the confidentiality, integrity and continued availability of critical information. The reliance on information and rapidly changing technology forces organizations to implement comprehensive information security programs to protect their information systems. However, the success of implementing such security programs relies largely on employees' awareness and compliance. The failure to secure information or to make it available when required to those who need it can, and does, lead to financial and non-financial losses (Abu-Musa, 2002).

Computer crime is almost inevitable in any organization unless adequate protections are put in place. The computer crime problem is no longer a local problem and security solutions cannot be viewed only from a national perspective. Computer crime and information security have expanded from relatively limited geographical boundaries to become worldwide issues. According to Williams (1995), any type of security breach, however minor, can become disruptive and expensive, so it must make better business sense to take a preventive approach. The sooner action is taken to safeguard information systems, the cheaper it will be for an

organization in the long run. Katz (2000) argued that maintaining security is a never-ending struggle. Just when one has an airtight system in place, a new hacker technology or an especially diabolical adversary enters the picture. The security threats are not necessarily external. In fact, the FBI Computer Crime Unit reports that more than 80 percent of all network security breaches are inside jobs by disgruntled or dishonest employees with their own agenda (Katz 2000, p. 12).

As automated accounting systems become more readily available to all types and sizes of businesses, the need to understand and employ adequate systems security becomes an issue no business owner can ignore (Henry, 1997). Nowadays most organizations, even the smallest, are capable of automating their accounting information systems in some form. Over the last several years, changes in technology have made computers much easier to use. However, user-friendly systems have created significant risks to the security and integrity of CAIS. West & Zoladz (1993) argued that although computers provide many benefits, inherent security issues of computerized systems are often not addressed by management. Many organizations might not realize the importance of their CAIS security until unauthorized modification to one of their sensitive files (such as a payroll file) or some other event occurs. Because information can be an organization's most valuable asset, leaving it unprotected is tantamount to underinsuring fixed assets or inventory. Organizations can no longer afford to ignore the importance of information security in the light of computer fraud, hackers and computer viruses.

The conversion from manual accounting information systems (MAIS) to CAIS achieves many advantages to an organisation, in the speed and accuracy of data processing as well as through the variety of accounting reports obtained. On the other hand, the radical change and rapid development in technology might create problems related to preserving CAIS security. Converting to CAIS creates new challenges regarding protecting these systems and the information that they contain against the various security threats and vulnerabilities. The security status of CAIS needs to be evaluated continually to determine the security gaps and weaknesses, so that appropriate security controls can be prescribed and implemented.

Qureshi and Siegel (1997) mentioned that there are daily reports in accounting and financial publications about computer related data errors, incorrect financial information, violation of internal controls, thefts, burglaries, fires and sabotage. Although considerable efforts have been made by practicing accountants to reduce vulnerability to such events, an increased effort is required. Moreover, there is a real need for organizations to investigate and understand the main threats that challenge their CAIS and to employ adequate safeguards to protect their automated accounting systems against the prospected security risks. Developing information security policy and enhancing employees' awareness regarding the information security are very important issues.

The objective of the current research is to explore the main characteristics of security policies of the computerized accounting information systems (CAIS) in the Egyptian banking industry (EBI), and to investigate whether there are any significant differences among different bank types regarding the existence, implementation, clarity, comprehensiveness, publicity, awareness, management attitudes, and participation in designing, developing and evaluating their banks' CAIS security policies and controls. The

Research Methodology

An empirical survey using a self-administered questionnaire has been conducted to investigate the opinions of the heads of internal audit departments (HoIAD) and the heads of computer departments (HoCD), in the entire population of the EBI, regarding the existence, implementation and the main characteristics of CAIS security policies. The questionnaire was pre-tested with PhD research students and staff in the Department of Accountancy at Aberdeen University, UK. Further, the questionnaire was pre-tested on selected members of academic staff and accounting practitioners during attendance at BAA / ICAEW Doctoral colloquia and at the BAA annual conference in 1999. Secondly, after considering the comments and suggestions of pre-test results, the revised questionnaire was piloted on a selected sample of bank branches in the EBI. Appropriate comments and suggestions were considered in developing and revising the final suggested questionnaire. The translation of

the questionnaire was tested by independent back-translation from the Arabic, showing close correspondence of the terminology and meaning of questions. Thus, questionnaire bias due to translation has been minimised.

The final revised questionnaire was used to survey the entire population of headquarters offices of the Egyptian banking sector regarding the above research issues. Two copies of the questionnaire were directed to each individual bank's headquarters. One was given to the head of the computer department and the other to the head of the internal audit department. Response was controlled by personal administration and collection by the researcher, minimising respondent bias.

In the first meeting, the researcher introduced himself to the target respondents; and gave them a brief introduction about his study and the main objectives of his research. The respondents were requested to fill up the questionnaire. Appointments were arranged with each individual respondent at their convenience for collecting the completed questionnaire and interviewing them. Interviewing the respondents as well as obtaining their business cards was the researcher's strategy to assure that the authorized and targeted respondents had completed the questionnaire by themselves. Therefore, a high degree of validity of their responses could be achieved, strengthening the reliability of the analysis and guarding against non-expert completion of the questionnaire. Sample and response bias have been rigorously controlled in this research.

Seventy-nine completed and usable questionnaires were collected, from forty-six different banks' headquarters. Forty-six of those questionnaires were completed by the heads of computer departments and thirty-three by the heads of internal audit departments. The response rate of the heads of computing departments (after excluding the banks that are already merged, liquidated, too remote, and non-computerized) was 79%. The response rate was 57% from the internal audit departments. Both can be considered a high response rate. The initial and revised banks' response rate according to the different banks' types are illustrated in the following table:

Table 1: The Response Rate of the Headquarters Sample

	Total N. of Banks		**Responded Banks**				**Respondents type**	
The Bank Type	Total N.	Net N.	Initial Rate		Revised Rate		Computers Dept.	Internal Audit Dept.
Commercial public bank	4	4	2	**50**%	2	**50**%	2	1
Specialized public bank	4	3*	2	**50**%	2	**66.7**%	2	2
Commercial private bank	23	22**	19	**82.7**%	19	**86.5**%	19	17
Joint venture bank	15	15	14	**93.4**%	14	**93.4**%	14	5
Branch of foreign bank	20	14***	9	**45**%	9	**64.3** %	9	8
Total	**66**	**58**	**46**	**69.7**%	**46**	**79.3** %	**46 (79.3%)**	**33 (56.9%)**

* 2 specialized public bank were merged in one bank

** One bank is too remote a region for access

*** 3 banks under liquidation

2 banks have non- computerized systems

1 bank the researcher was not able to meet the target respondents within the period scheduled for the survey

The main results and statistics of the current research are presented in the following sections

Security Policies of Cais

In order to explore the respondents' opinions regarding the current state of their accounting information systems' security policies the respondents were asked to express their opinions by circling one number from a seven-point Likert scale, in which number one refers to very poor security policy and seven indicates that the security policy is exceptional. The statistical results revealed that 62 percent of the respondents asserted that the security policies in their banks are either "strong" or "very strong" (38 percent and 24 percent respectively). A

further 23 percent of the respondents considered their banks' security policies "almost strong". Approximately 14 percent of respondents believed that the security policies in their banks were "adequate". Only 1.3 percent of the respondents evaluated their banks' security policies as almost poor. In general, 85 percent of the respondents agreed (in varying degrees) that their banks had "strong" security policies.

The statistical results of the Kruskal-Wallis test (Appendix 2) and the one-way ANOVA test (Appendix 3) provide strong evidence that there is a significant difference among different bank types regarding respondents' opinions on the current, implemented CAIS security policies in the EBI (at significant level p = 0.05). However, according to the Mann-Whitney test (Appendix 1), it seems that there were no significant differences between the HoCDs' and HoIADs' points of view regarding current implemented CAIS security policies (at significance level p = 0.05).

To explore further whether there is any relationship between the security policy status and the bank types a cross-tabulation of responses was performed. The statistics reveal that one of the two commercial public banks asserted that their security policy was "very strong", while the other evaluated it as "strong". One the other hand, one specialized public bank believed that the banks' security policy was "almost strong", while the other considered it "adequate". The great majority of commercial private banks asserted that their banks' security policies were in some way "strong". Approximately 90 percent of them reported their security policies to be either "very strong" (21.1 percent); "strong" (42.1 percent); or "almost strong" (26.3 percent).

Half of the joint venture banks considered their security policies to be either "strong" or "very strong", while 21.4 percent of them believed that their security policies were "almost strong" and a similar proportion considered them "adequate". On the other hand one of the joint venture banks asserted that the bank's security policy was "very poor". Almost 56 percent of the local headquarters of foreign banks considered their banks' security policies as "strong", while 22.2 percent of them evaluated them as "very strong".

In an attempt to eliminate the effect of a double-weighting problem on the results obtained, further analysis was carried out on the forty-six banks. In contrast with the above results, the statistical finding of both the one- way ANOVA (Appendix 6) and the Kruskal-Wallis tests (Appendix 4) revealed non-significant differences among different bank types regarding their current implemented CAIS security policies (at significance level p =. 05). Moreover, in order to explore whether there were any significance differences between the HoCD and the HoIAD related to the current CAIS security policies implemented in their banks, a further cross-tabulation was done. In an attempt to eliminate the effect of bank type, the thirteen banks with a sole respondent were excluded from the analysis. However, after eliminating the effect of bank type, the statistical results of the Mann-Whitney results still supported non-significant differences between the two respondent groups (at p = 0.05) (Appendix 5).

The Existence of Formal Written Security Policies

To investigate the respondents' opinions regarding the existence of formal written security policies in their banks, the respondents were asked to indicate whether their banks had formal written security policies for the CAIS currently in place. The statistical results show that almost 75 percent of the respondents had formal written security policies in their banks and only 9 percent of the respondents believed that there were no formal written security policies in their banks. However, 16.5 percent of respondents were not sure whether there were formal security policies in their banks or not.

Again, the statistical results of the Kruskal-Wallis (Appendix 2) and the one-way ANOVA test (Appendix 3) show a significant difference among different bank types regarding the existence of formal written security policies (at significance level p = 0.05). On the other hand, the statistical finding of Mann-Whitney test (Appendix 1) does not support significant differences between the opinions of the HoCD and HoIAD related to the existence of formal written security policies in their banks (at significance level p = 0.05).

The statistical findings revealed that all of the commercial public banks' respondents asserted that their

banks had formal written security policies, while 50 percent of specialized public banks' respondents indicated that their banks had no formal written security policies in place and the other half were not sure whether such security policies existed in their banks or not. The findings also revealed that approximately 95 percent of the commercial private banks' respondents reported the existence of formal written security policies in their banks. The majority of respondents from the joint venture banks (64.4 percent) and of the local headquarters of foreign banks (77.8 percent) asserted the existence of formal written security policies in their banks. Consistent with the obtained results, both the Kruskal-Wallis test (Appendix 4), and the one- way ANOVA (Appendix 6) provided further evidence that there were significant differences among the different bank types regarding the existence of formal written security policies in their banks (at significance level $p = 0.05$).

The results shows 29 of the HoCD (88 percent) reported the existence of formal written security policies in their banks, while only 23 of the HoIAD (approximately 70 percent) did so. Consisting with this finding, the result of the Mann-Whitney test (Appendix 5) showed non-significant differences between the opinions of the two respondent groups regarding the existence of formal written security policies in their banks (at significance level $p = 0.05$).

Clarity and Comprehensiveness of Security Policies

The main objective at this point is to explore respondents' opinions regarding the clarity and comprehensiveness of their banks' security policies. The statistical results show that approximately 34 percent and 33 percent of the total respondents respectively "agreed" and "strongly agreed" that their banks had clear and comprehensive CAIS security policies. Moreover, another 11.4 percent of the respondents "almost agreed" that their banks' security policies are clear and comprehensive, while 15.2 percent of them were neutral. On the other hand, 5 percent of the respondents "almost disagreed" and 1.3 percent "strongly disagreed" that their banks had clear and comprehensive security policies. The statistical results of both the Kruskal-Wallis (Appendix 2) and the one-way ANOVA (Appendix 3) tests strongly support the existence of significant differences among different bank types regarding the clarity and comprehensiveness of their security policies (at $p = 0.05$). At the same time, the Mann-Whitney test (Appendix 1) suggests non-significant differences between the HoCDs' and HoIADs' points of view about the clarity and comprehensiveness of their banks' security policies (at significance level $p = 0.05$).

To explore the relationship between the clarity and comprehensiveness of security policies and the bank types, a cross tabulation was performed. The statistics indicate that one of the two commercial public banks "agreed" that its security policy is clear and comprehensive; while the other was "neutral". In contrast, both of the specialized public banks' respondents were neutral. The majority of the commercial private banks (some 90 percent) either "strongly agreed" (31.6 percent) or "agreed" (58 percent) that their banks had clear and comprehensive security policies. It was observed that eight of the joint venture banks (57 percent) either "agreed" or "strongly agreed" with this statement. Finally, the majority of the local headquarters of foreign banks (89 percent) somewhat "agreed" that they had clear and comprehensive security policies in place. It is interesting to note that, after eliminating the effect of double weighting problem by performing the analysis on the forty six banks as unique observations, the statistical results of both the one-way ANOVA (Appendix 6) and the Kruskal-Wallis tests (Appendix 4) report non-significant differences among different bank types regarding the clarity and comprehensiveness of security policies in place (at $p = 0.05$).

To investigate whether there is any relationship between the respondent types and the clarity and comprehensiveness of security policies, a further cross-tabulation was carried out. The finding tends to suggest, again, that the great majority of both groups agreed that their banks' security policies were clear and comprehensive. The finding also tends to suggest that there were no significant differences between the two respondent groups. The result of the Mann-Whitney test provides empirical support for this non-significance of differences between the two respondent groups (at $p = 0.05$: Appendix 5).

Reasonableness of Security Policies

"Reasonableness" directs the respondents' attention to fitness for purpose. In an attempt to understand the reasonableness of the security policies in the EBI the respondents were asked to indicate their opinions by circling one number on a seven-point Likert scale. The results shows, approximately 23 percent of the total respondents "agreed" and 35.4 percent of them "strongly agreed" that their banks' security policies were reasonable. A further 19 percent of respondents "almost agreed" that their banks' security policies were reasonable. On the other hand, a mere 5 percent "almost disagreed" that their bank security policies were reasonable. However, 17.7 percent held "neutral" opinions.

The statistical results of both the Kruskal-Wallis (Appendix 2), and the one-way ANOVA (Appendix 3) tests show significant differences among different bank types regarding the reasonableness of security policies implemented in their banks (at significance level $p = 0.05$). While, the statistical finding of the Mann-Whitney test (Appendix 1) shows no significant differences between the opinions of the HoCD and HoIAD related to the reasonableness of their banks security policies (at significance level $p = 0.05$).

Again the results indicate that one of the commercial public banks "strongly agreed" that its security policy was reasonable, while the other was "neutral". On the other hand, both of the specialized public banks were "neutral". The results also revealed that two respondents of the commercial private banks "almost agreed", six "agreed", and eight "strongly agreed" that their banks had reasonable security policies. In joint venture banks three respondents "almost agreed", three respondents "agreed" and four "strongly agreed" that their banks had reasonable security policies. On the other hand, two of the joint venture banks "almost disagreed" and two of them were "neutral". Five local headquarters of the foreign banks "strongly agreed", two of them "agreed" and one "almost agreed".

After considering the effect of double weighting problem, In contrast with the above the statistical results, both the Kruskal-Wallis test (Appendix 4) and the one-way ANOVA test (Appendix 6) revealed non-significant differences among the different bank types regarding the reasonableness security policies in their banks (at significance level $p = 0.05$). The result of the Mann-Whitney test (Appendix 5) provides further support that there are no significant differences between the opinions of respondent types regarding the reasonableness of their banks' security policies (again at significance level $p = 0.05$).

Publicity Of Security Policies

The statistical findings revealed that 31.6 percent of the total respondents "agreed" and 34.2 percent of them "strongly agreed" that their banks' security policies were well published and well known by users. Moreover, 24.1 percent of the total respondents "almost agreed" with the previous opinion. Only one respondent did not agree that his / her bank had a clear and well-published information security policy (seven respondents were "neutral"). The statistical results of both the Kruskal-Wallis (Appendix 2), and the one-way ANOVA (Appendix 3) tests demonstrate a significant difference among different bank types regarding the publicity of their security policies (at significance level $p = 0.05$). The Mann-Whitney test (Appendix 1) does not show any significant differences between the opinions of the HoCD and HoIAD related to the publicity of their banks' security policies (at $p = 0.05$).

To explore any relationship between the publicity of the security policies and the different bank types a cross tabulation was carried out. It appears that one of the two commercial public banks "strongly agreed" that it had a clear and well-published security policy, while the other was "neutral". Again, one of the specialized public banks "almost agreed" that its security policy was well published, while the other was "neutral". It generally appears that the respondents of the specialized public banks were dissatisfied regarding the publicity of their banks' security policies. Nine of the commercial private banks (47.4 percent) "strongly agreed" and eight (42.1 percent) "agreed" that they had well published security policies to users; and two further respondents (10.5 percent) "almost agreed".

Five of the joint venture banks "almost agreed", four "agreed" and three "strongly agreed" that their banks had well published security policies. On the other hand, only one joint venture bank respondent regarded

its security policy as not well published, while another was "neutral". Finally, two thirds of the foreign banks' local headquarters "strongly agreed", while the other third "agreed" that their banks had well published security policies.

After considering the double weighting problem (by performing the data analysis on the HoCD of the forty-six banks), the results of both the Kruskal-Wallis test (Appendix 6) and the one-way ANOVA test (Appendix 6) still support the existence of significant differences among different bank types regarding the publicity of their security policies (at p = 0.05). Turning to differences by respondent function, the results showed that the HoIAD had a higher-ranking score related to the publicity of their bank security policies when compared with the HoCD. Moreover, after eliminating the effect of bank type by conducting the analysis on the 33 banks with both HoIAD and HoCD responding, the statistical results of the Mann-Whitney test (Appendix 5) provide strong evidence that the differences between the two respondent groups are very significant (in this case at p = 0.003).

Awareness of Cais Security Policies

To explore the respondents' opinions regarding the general awareness of their banks' security policy, the respondents were asked to indicate their opinion about the awareness of CAIS security issues of their banks' managers as well as of employees. The statistical results indicated that thirty-six of the respondents (approximately 46 percent of the total respondents) "agreed" or "strongly agreed" (almost 23 percent each) that their banks' managers and employees had adequate awareness regarding CAIS security issues. Moreover, another fourteen respondents (17.7 percent) "almost agreed" with the previous opinion. On the other side, five respondents "disagreed" and four "strongly disagreed" that their banks' managers and employees had adequate awareness related to CAIS security issues. Seven respondents - representing 9 percent of the total respondents - had "neutral" opinions. The results of both the Kruskal-Wallis (Appendix 2) and the one-way ANOVA (Appendix 3) tests tend to suggest that there are no significant differences among different bank types regarding the total awareness of the CAIS security issues (at p = 0.05). Furthermore, the Mann-Whitney test (Appendix 1) revealed non-significant differences between the opinions of the HoCD and the HoIAD (at significance level p = 0.05).

However, a cross-tabulation carried out on the forty-six individual banks to explore the relationship between the total awareness the CAIS security issues and bank types indicated that one commercial public bank "strongly agreed" that its managers and employees had adequate awareness of security issues, while the other held a "neutral" opinion. On the other hand, one specialized public bank "almost agreed" with the adequacy of its managers and employees' awareness of security issues and the other was "neutral". The results also indicated that slightly more than half of commercial private banks' respondents (approximately 58 percent) agreed to some degree that there was adequate awareness of security among their banks' managers and employees. In contrast, five commercial private bank respondents (26.3 percent) disagreed. Respondents in nine joint venture banks (64.3 percent) supported the adequacy of general awareness of information security among their employees and staff, while two disagreed with this opinion. The result also shows that the vast majority of respondents from foreign banks' local headquarters (approximately 89 percent) believed in the adequacy of awareness regarding the security issues in their banks.

Both the Kruskal-Wallis test (Appendix 4), and the one-way ANOVA test (Appendix 6) provide further evidence that there are no significant differences among the different bank types regarding the general awareness of CAIS security issues (at significance level p = 0.05). Again, a cross-tabulation was carried out on the 33 pairs of respondents to explore whether there were significant differences between them, after eliminating the effect of banks' type on the results. The statistics show that the HoCD had higher ranking scores related to the general awareness of CAIS security issues when compared with the HoIAD. However, the Mann-Whitney test (Appendix 5) indicated that these differences are non-significant (at significance level p = 0.05).

Attitudes Toward Cais Security Policies

Respondents were asked to indicate whether their managers' attitudes toward the security of the banks' CAIS were serious and whether their managers paid sufficient attention to security issues. The statistical results revealed that sixty-one respondents (77.2 percent of the total responses) believed that managers had positive attitudes and paid great attention to security issues. Only five respondents (6.3 percent) disagreed with the previous opinion, with thirteen respondents (16.5 percent) neutral. The statistical results of both Kruskal-Wallis (Appendix 2) and one-way ANOVA (Appendix 3) tests show significant differences among different bank types regarding their managers' attitudes toward the security of CAIS (at $p = 0.05$). On the other hand, the statistical result of the Mann-Whitney test (Appendix 1) suggests that differences between the opinions of the HoCD and HoIAD regarding managers' attitudes toward the security of CAIS in their banks are not significant (at $p = 0.05$).

To explore whether there is any relationship between the managers' attitudes toward the security issues and the different bank types, a cross- tabulation of the responses was performed on these variables. The results revealed that the respondents of both commercial public banks and specialized public banks had "neutral" opinions regarding the attitudes of their banks' managers towards CAIS security. In commercial private banks, the vast majority of these respondents (84.2 percent) considered the attitudes of their managers regarding the security issues to be positive, while the others had neutral opinions. It is also observed that the majority of both the joint venture banks (almost 71.4 percent) and all foreign bank respondents asserted the positive attitudes of their managers toward the information security issues.

Both the Kruskal-Wallis test (Appendix 4) and the one-way ANOVA test (Appendix 6) reported significant differences among the different bank types related to their managers' attitudes toward security issues (at significance level $p = 0.05$). Moreover, the cross-tabulation 10-3-21 shows that twenty-seven of the HoCD (approximately 82 percent) supported the positive attitudes of their managers toward CAIS security issues, while 26 of the HoIAD (approximately 79 percent) supported that point of view. This finding tends to suggest that the HoCD displayed more positive perception regarding their managers' attitudes toward security issues, compared with the HoIAD. There is no strong statistical support for this, however. The result of the Mann-Whitney test (Appendix 5) provides empirical evidence that there are no significant differences between the opinions of the two groups regarding their managers' attitudes toward CAIS security issues (at $p = 0.05$).

Participation in Designing Cais Security Controls

In an attempt to understand the participation of the HoCD and the HoIAD in designing their banks' CAIS security controls, the respondents were asked to indicate whether they actually took part and whether their opinions were considered in the design stage of their banks' security controls. More than 68 percent of respondents agreed to some degree that they participated in design of their banks' security controls and that their opinions were seriously considered. In contrast, 20.3 percent of respondents indicated that they had never participated in designing their banks' security controls and that their opinions were never considered in that area. 11.4 percent of respondents expressed neutral opinions.

The statistical results of Kruskal-Wallis (Appendix 2) and the one-way ANOVA test (Appendix 3) report no significant difference among different bank types regarding the respondents' participation in designing their security controls (at significance level $p = 0.05$). Furthermore, the Mann-Whitney test (Appendix 1) shows non-significant differences between the opinions of the HoCD and HoIAD (at $p = 0.05$).

The results appeared that one commercial public bank respondent strongly confirmed the participation of the HoCD in designing the banks' security controls, while none of the specialized public banks' respondents took part. The statistics shows that slightly more than half of the commercial private banks' respondents (58 percent) participated in the designing of security controls. Moreover, more than 78 percent of respondents in the joint venture banks and all respondents of foreign banks asserted that they participated.

While the statistical result of the Kruskal-Wallis test (Appendix 4) shows significant differences among bank groups (at $p = 0.021$), the finding of the one-way ANOVA test (Appendix 6) displays no significant differences among the different bank types (at significance level $p = 0.05$). However, to investigate whether there

is any relationship between the two respondent groups in their participation in designing the banks' security controls, a cross-tabulation was carried out. The result tends to suggest that the majority of both groups reported participation in designing their banks' security controls. Although the HoCD had a higher rank score for their participation in designing security controls, compared with the HoIAD, the Mann-Whitney test results reveal non-significant differences between the two respondents' groups (at $p = 0.05$).

Development of Cais Security Controls

In order to explore the respondents' participation in developing the implemented CAIS security controls, respondents were asked to indicate whether their suggestions and opinions concerned with developing CAIS security were respected and considered. The results show that a majority of the participating respondents (64.6 percent) agreed that they participated in developing the security control of CAIS in their banks and that their opinions and suggestions were considered. In contrast, thirteen respondents (16.4 percent) indicated that they never participated in developing their banks' CAIS security controls and, therefore, their opinions and suggestion were rarely considered. Another 19 percent of respondents had "neutral" opinions.

The results of both the Kruskal-Wallis (Appendix 2) and the one-way ANOVA test (Appendix 3) show non-significant differences among different bank types (at significance level $p = 0.05$). According to the Mann-Whitney test (Appendix 1), it also seems that there are no significant differences between the HoCDs' and HoIADs' points of view (at significance level $p = 0.05$).

The statistical findings tend to suggest that all the commercial public banks agreed that they participated in developing their security control systems. On the other hand, only one respondent in the specialized public banks expressed agreement, while the other had a neutral opinion. The findings also reveal that more than half of the commercial private banks' respondents (approximately 58 percent) and a similar proportion of joint venture banks' respondents (57 percent) confirmed their participation in developing their banks' CAIS security controls. On the other hand, all respondents in the local headquarters of foreign banks indicated agreement.

In an attempt to exclude the possible effect of a double weighting problem on the obtained statistical results, further analysis was conducted on the forty-six individual banks. In contrast with the above findings, the results of both the Kruskal-Wallis (Appendix 4) and the one-way ANOVA (Appendix 6) tests strongly support the existence of significant differences among the different bank types (at significance level $p = 0.05$). Further, to explore any significant differences between the HoCD and the HoIAD, a cross-tabulation was performed. It seems that there is some difference between the opinions of the two respondent groups regarding their participation in developing the implemented security controls in their banks. The Mann-Whitney test result (Appendix 5) provides empirical evidence of this significance (at $p = 0.041$).

Evaluations of Cais Security Controls

The objective of this question was to explore whether respondents paid due attention to security controls in their evaluation of CAIS. The statistics indicates that the majority of respondents (82.3 percent) claimed to pay considerable attention to security controls in evaluation. Approximately 4 percent of respondents appeared to ignore security controls in their evaluation of CAIS and approximately 14 percent had neutral opinions. Both the Kruskal-Wallis (Appendix 2) and the one-way ANOVA (Appendix 3) tests revealed a significant difference among different bank types (at significance level $p = 0.05$). On the other hand, the result of Mann-Whitney test (Appendix 1) does not support the significance of differences between the opinions of the HoCD and HoIAD regarding that issue (again at $p = 0.05$).

To explore whether there is any relationship between respondents' perception and the different bank types, a cross-tabulation of the responses was performed. The statistical results indicated that one commercial public bank respondent strongly confirmed attention to security controls in evaluating CAIS, while only one of the specialized public banks' respondents did so. The results also revealed that the great majority of respondents in the commercial private banks (89 percent) and joint venture banks (approximately 79 percent), and all

respondents in the local headquarters of foreign banks, claimed to consider security controls during their evaluation of CAIS.

Consistent with the above result, both the Kruskal-Wallis test (Appendix 4) and the one-way ANOVA test (Appendix 6) provide further support of significant differences among different bank types ($p = 0.009$). Approximately 85 percent of the heads of computer departments confirmed that they paid considerable attention to the security controls as a critical element in evaluating CAIS. In contrast, some of the heads of internal audit departments (79 percent) indicated that they seriously considered security controls in their evaluation. After eliminating the effects of bank types, the Mann-Whitney test (Appendix 5) supports the significance of differences between the opinions of the two respondent groups regarding their consideration of security controls in the evaluating the banks' CAIS ($p = 0.041$).

Total Awareness of Cais Security Issues

To explore the general awareness of information security issues in the respondent banks, respondents were asked to indicate whether they believed that their managers and employees had adequate awareness of the bank's CAIS security issues. The statistical results suggest that the majority of respondents (77.2 percent) believe that their managers and banks' employees had adequate awareness. However, a minority (almost 9 percent) believed that awareness of security issues was inadequate; and approximately 14 percent of the respondents held neutral opinions. Both the Kruskal-Wallis test (Appendix 2) and the one-way ANOVA test (Appendix 3) tend to suggest that there are no significant differences among different bank groups regarding the general awareness of information security issues among their managers and employees (at significance level $p = 0.05$). On the other hand, the Mann-Whitney test (Appendix 1) reports significant differences between the two respondent groups (at $p = 0.006$).

To explore any relationship between the bank type and the total awareness of security issues, cross-tabulation of the responses was performed. The results indicate that all the commercial public banks' respondents agreed that there was adequate awareness. On the other hand, one of the respondents in the specialized public banks believed that it had adequate awareness, while the other had a neutral opinion. The results also revealed that sixteen of the commercial private bank respondents (84 percent) and eleven of those in joint venture banks (79 percent) believed that they had adequate awareness of CAIS security issues, while all respondents in the foreign banks' local headquarters believed that they had adequate security awareness. Again, the statistical findings of both the Kruskal-Wallis test (Appendix 4) and the one-way ANOVA test (Appendix 6) indicate the non-significance of any differences among different bank types (at significance level $p = 0.05$).

Returning to the two respondent groups, it seems that the majority of the HoCD (approximately 88 percent) believed that their banks' managers and employees had adequate awareness of the security issues, as did two thirds of the HoIAD. Consistent with the result above, the Mann-Whitney test (Appendix 5) provides further evidence of the significant differences between the HoCD and HoIAD (here at $p = 0.004$).

Respondent's Own Awareness Of Cais Security Issues

In relation to the respondents' awareness of security controls, respondents were asked directly to indicate the degree of their awareness of their banks' CAIS security issues. More than 91 percent of the sample confirmed their awareness of their CAIS security issues. Only one respondent believed that he was almost unaware of security issues, and 6 respondents (7.6 percent) had neutral opinions. The results of the Kruskal-Wallis (Appendix 2) and one-way ANOVA (Appendix 3) tests show significant differences among different bank groups regarding the respondents' awareness of security issues (at significance level $p = 0.05$). While, the Mann-Whitney test (Appendix 1) revealed non-significant differences between the HoCD and HoIAD (at $p = 0.05$).

The results also show that all the commercial public banks' respondents confirmed their awareness of CAIS security issues, while only 50 percent of the specialized pubic banks' respondents believed that they had

adequate awareness. Similarly, the vast majority of the private commercial banks' respondents (almost 95 percent) and almost 86 percent of the joint venture banks' respondents confirmed their awareness of security issues, while all respondents of the local headquarters of foreign banks believed that they were strongly aware of their banks' security issues. Consistent with the above result, after eliminating the effect of respondent types on the prospected results, the findings of both the Kruskal-Wallis test (Appendix 4), and the one-way ANOVA (Appendix 6) show significant differences among the different bank types related to their respondents' awareness of security issues (at significance level $p = 0.05$). However, after eliminating the potential effect of bank types on the obtained results, the Mann-Whitney test (Appendix 5) suggests significant differences of security awareness between the two respondent groups (at significance level $p = 0.041$).

Unauthorized Accesses To Cais

To explore the respondents' opinions regarding the penalties that should be imposed against those who intentionally abuse the banks' CAIS and access it in unauthorised ways, respondents were asked whether the relevant acts should be classed as a felony, misdemeanour, or merely merit a warning. The responses reveal that approximately 66 percent of the respondents considered such action as a crime and that in determining penalties, it should be regarded as a felony. However, 21.5 percent of the respondents believed that unauthorised access should be considered as a misdemeanour. A minority of respondents (12.7 percent) believed that the penalty should be just a warning, especially if unauthorised access was gained internally by an employee, in order to carry out legitimate work under certain limitations. The results of both the Kruskal-Wallis test (Appendix 2) and the one-way ANOVA test (Appendix 3) tend to suggest that there are no significant differences among different bank groups regarding penalties that should be taken (at $p = 0.05$). Moreover, the Mann-Whitney test (Appendix 1) displays non-significant differences between the HoCD and the HoIAD related to penalties (at significance level $p = 0.05$).

The statistics show that one commercial public bank considered unauthorised access as a felony and the other considered it as a misdemeanour. The respondents from specialized public banks were equally divided regarding prospective penalties: 50 percent of them considered the action as a felony, while the other half believed that it is a misdemeanour. A relatively high proportion of the respondents of foreign bank local headquarters (77.8 percent), joint venture banks (64.3 percent) and commercial private banks (approximately 58 percent) considered unauthorised access to the banks' accounting systems as a felony. Again, after considering the potential effect of respondent type on the results obtained, the statistical findings of both the Kruskal-Wallis test (Appendix 4) and the one-way ANOVA (Appendix 6) are consistent with the above results. They provide further support that there are no significant differences among different bank groups regarding penalties that should be imposed (at $p = 0.05$).

The majority of the heads of computer departments (73 percent) believed that unauthorised access to the banks' accounting systems is a crime and should be treated as a felony. A minority (18 percent) considered that action as a crime, but suggested that it should be treated as a misdemeanour. The remainder believed that the penalty should be just a warning. For the heads of internal audit departments, approximately 70 percent consider unauthorised access to the accounting systems as a crime to be prosecuted as a felony. A minority (18 percent) agreed that this action is a crime, but they suggested that it should be treated as a misdemeanour. Only 12 percent of the internal auditor respondents believed that the penalty could be only a warning. After considering the potential effect of bank types on the results obtained, the Mann-Whitney test (Appendix 5) still supports the above results and indicates non-significant differences between the two groups regarding the penalties that should be imposed (at $p = 0.05$).

Intentional Manipulations Of Banks' Data And Records

To explore respondents' opinions regarding the appropriate penalties against those who intentionally destroy, copy or alter any of the bank data and records, respondents were asked again whether they believe the action should be classed as a felony, or misdemeanour, or merely warrant a warning. The results indicate that the vast majority of the respondents (approximately 90 percent) believed that this action is also a crime and

should be prosecuted as a felony. The remainder of the respondents (10 percent) agreed that the action is a crime, but considered it as a misdemeanour rather than a felony.

According to the statistical results of both Kruskal-Wallis (Appendix 2), and one-way ANOVA (Appendix 3) tests, no significant differences have been uncovered among different bank groups regarding the penalties that should be imposed (at p = 0.05). Again, the result of the Mann-Whitney test (Appendix 1) shows no significant differences between the two respondent groups about the penalties that should be imposed for unauthorized access (at p = 0.05).

The statistics revealed that all respondents in commercial and specialized public banks and the local headquarters of foreign banks considered intentional destruction, manipulation or alteration of the banks' records as a felony. Moreover, the vast majority of respondents in commercial private banks (89.5 percent) and joint venture banks (approximately 79 percent) agreed. Again, the results of both the Kruskal-Wallis test (Appendix 4) and the one-way ANOVA test (Appendix 6) show non-significant differences among the different bank types (at significance level p = 0.05). It is also observed that more than 90 percent of both HoCD and HoIAD groups believe that the intentional destruction, manipulation, or alteration of the banks' accounts and records is a felony. It is very interesting to notice complete agreement between the two groups relating this issue.

Unintentional Manipulations Of Banks' Data And Records

Turning to unintentional manipulation of data and records, respondents were asked to indicate their opinions about the appropriate action against such threats. The great majority of the respondents (almost 95 percent) considered that action to be a crime and that prosecution should follow against whosoever committed it. Only three respondents believed that this action should be treated as a misdemeanor rather than a felony. Finally, only one respondent believed that a warning would be the adequate response. The Kruskal-Wallis (Appendix 2) and the one-way ANOVA tests (Appendix 3) indicate non-significant differences among different bank types regarding the penalty here (at p = 0.05). On the other hand, the statistical finding of the Mann-Whitney test (Appendix 1) displays significant differences between the two respondent groups (at significance level p = 0.040).

In terms of bank type, every respondent of the commercial public banks, specialized public banks and local headquarters of foreign banks agreed that indirect destruction and manipulation of banks' data and records is a crime and that anyone who commits such a crime should be prosecuted. The vast majority of the commercial private banks' respondents (84 percent) and the joint venture banks' respondents (approximately 93 percent) also considered the destruction or even the manipulation of the banks' accounts and records indirectly as criminal and to be treated as a felony, while the remainder believed that this action should be considered as a misdemeanor.

Again, both the Kruskal-Wallis test (Appendix 4) and the one-way ANOVA (Appendix 6) provide further support of the above result. The results suggest that there are no significant differences among different bank types regarding the action that should be taken (at significance level p = 0.05). The statistical results also suggest that there is complete agreement among the heads of internal auditors that the action should be treated as a felony. The great majority (almost 91 percent) of the heads of computer departments supported this opinion, while a minority of them (9 percent) believed that such action should be considered as a misdemeanor. After eliminating the potential effect of bank types on the obtained results, the Mann-Whitney test (Appendix 5) confirms the non-significance of differences between the two respondent groups (again at significance level p = 0.05).

Conclusions

This paper has provided an understanding of some of the characteristics of CAIS security policies in the EBI. Differences among bank types regarding the existence, implementation, clarity, comprehensiveness, publicity, awareness, management attitudes, and participation in designing, developing and evaluating their banks' CAIS security policies have been explored. Furthermore, differences between the opinions of the HoCD

and HoIAD related to CAIS security policies have been investigated. Based on the results obtained, it seems that the vast majority of respondents asserted that their banks have formal written, clear, comprehensive, reasonable and well-published CAIS security policies. Moreover, the majority of respondents believed that there was adequate awareness of CAIS security issues among their banks' managers and employees and that managers had positive attitudes and paid great attention to security issues. Further, the majority of respondents also claimed that they participated in designing, developing and evaluating their banking CAIS security controls.

References

1. Abu-Musa, Ahmad A. (2002), "Computer Crimes: How Can You Protect Your Computerized Accounting Information Systems", *The Journal of American Academy of Business, Cambridge, USA*, Vol. 2. No.1 September 2002, pp. 91-111.
2. Davis, Charles E. (1996), "Perceived Security Threats to Today's Accounting Information Systems: A Survey of CISAs", *IS Audit & Control Journal*, (Vol. 3), pp. 38 - 41.
3. Henry, Laurie; (1997), "A Study of The Nature And Security of Accounting Information Systems: The Case of Hampton Roads, Virginia", *The Mid-Atlantic Journal of Business*, (Vol. 33, Iss. 63), pp. 71-189.
4. Lee, Chi-Lin (1995), "A Study Of Financial Institutions, Information Security: Factors That Influence Employees, Willingness To Adhere To Information security procedures ", *DBA (ADAI) Dissertation*, (June) pp. 1-153.
5. Loch, Karen D., Houston H. Carr and Merrill E. Warkentin (1992), "Threats to Information Systems: Today's Reality, Yesterday's Understanding", *MIS Quarterly*, (December), pp. 173 - 186.
6. Qureshi, Anique A and Joel G Siegel (1997), "The accountant and computer security", *The National Public Accountant*; Washington, May.
7. Rockwell, Robin (1990), "The Advent of computer -related Crimes", *Secured lender (SCL)*, (Jul /Aug), pp. 40-42.
8. Roufaiel, Nazik S. (1990), "Computer Related Crimes: An Educational and Professional Challenge", *Managerial Auditing Journal*, (Vol. 5 Iss. 4), pp. 18 - 25.
9. Sherizen, Stanford (1992), "The Globalization of Computer Crime and Information Security", *Computer Security Journal*, (Fall), pp. 13-19.
10. Williams, Paul (1995), " Safe, Secure and up to Standard", *Journal of Accountancy*, (Apr. 1990) p. 60.

Your Professional Experience

(Please, tick the appropriate answer for each of the following questions)

1. Do you currently work in: (Please, tick)
   - ❒ **Public Sector Bank**
     - ❒ Commercial Bank
     - ❒ Specialized Bank
   - ❒ **Private Sector Bank**
     - ❒ Commercial Bank
     - ❒ Business & Investment Bank
       - ❒ *Private or Joint bank*
       - ❒ *Offshore bank*

2. How many accountants are employed and working in accounting tasks in your bank?
   - ❒ 1- 250
   - ❒ 251 - 500
   - ❒ 501 - 1000
   - ❒ 1001 - 2000
   - ❒ More than 2000

3. How many information system specialists are employed in your bank?
   - ❒ 1 - 10
   - ❒ 11 - 25
   - ❒ 26 - 50
   - ❒ 51 - 100
   - ❒ 101 - 200
   - ❒ More than 200

4. How many years of experience do you have at your current position in this bank?
   - ❒ 1 - 5
   - ❒ 6 - 10
   - ❒ 11 - 15
   - ❒ 16 - 20
   - ❒ 21 - 25
   - ❒ More than 25 years

5. How many total years of accounting/auditing experience do you have?
   - ❒ 1 - 5
   - ❒ 6 - 10
   - ❒ 11 - 15
   - ❒ 16 - 20
   - ❒ 21 - 25
   - ❒ More than 25 years

6. What highest education level do you hold? (Please, tick)
   - ❑ High school
   - ❑ Vocational school
   - ❑ Some college
   - ❑ Other - please specify _____
   - ❑ College Graduate
   - ❑ Diploma
   - ❑ Master degree

7. The net assets value in your bank for the last year were ------- bn (actual number); or
   - ❒ < .5 bn
   - ❒ .5 bn - 1 bn
   - ❒ 1 bn - 2 bn
   - ❒ 2 bn - 4 bn
   - ❒ More than 4 bn

8. How many full-time employees, including managers, does your bank employ?
   - ❒ 1 - 300
   - ❒ 301 - 600
   - ❒ 601 -1200
   - ❒ 1201 - 2400
   - ❒ More than 2400

Assessment of Your Bank's Accounting Information Systems Security Policies

The main objective of this part of the questionnaire is investigating your opinions regarding certain issues of your bank's headquarters accounting information systems security programs or policies.

*Please circle **one** number for each question:*

1. In your opinion, your bank's current accounting information systems security policies are:

Very poor				Adequate			Very strong
1	2	3	4	5	6	7	

2. Does your bank have formal written policies for the accounting information systems security currently in Place?

❑ **Yes** ❑ **No** ❑ **Don't Know**

3. Your bank's current accounting information systems security policies are clear and comprehensive.

Strongly disagree			Neutral			Strongly agree
1	2	3	4	5	6	7

4. Your bank's current accounting information systems security policies are reasonable.

Strongly disagree			Neutral			Strongly agree
1	2	3	4	5	6	7

5. Your bank's current accounting information systems security policies are well published for its users.

Strongly disagree			Neutral			Strongly agree
1	2	3	4	5	6	7

6. Your bank has an adequate accounting information systems security awareness-training program for its computer users.

Strongly disagree			Neutral			Strongly agree
1	2	3	4	5	6	7

7. Your manager's attitude toward the accounting information systems security is serious and he / she pay a great attention to this issue.

Strongly disagree			Neutral			Strongly agree
1	2	3	4	5	6	7

8. You participate in designing the accounting information systems security controls and your suggestions and opinions that concerned with the accounting systems security issue are respected and considered.

Strongly disagree			**Neutral**			**Strongly agree**
1	**2**	**3**	**4**	**5**	**6**	**7**

9. Your suggestions and opinions concerning with development of the accounting information systems security are respected and considered during the systems implementation.

Strongly disagree			**Neutral**			**Strongly agree**
1	**2**	**3**	**4**	**5**	**6**	**7**

10. You pay considerable attention to the information security controls in your evaluation of the computerized accounting information systems.

Strongly disagree			**Neutral**			**Strongly agree**
1	**2**	**3**	**4**	**5**	**6**	**7**

11. Your bank's manager and employees have adequate awareness of accounting information systems security issue.

Strongly disagree			**Neutral**			**Strongly agree**
1	**2**	**3**	**4**	**5**	**6**	**7**

12. Please indicate the degree of your awareness of the bank's accounting information systems security program.

Strongly unaware			**Neutral**			**Strongly aware**
1	**2**	**3**	**4**	**5**	**6**	**7**

13. In your view, if someone were to gain unauthorized access to the bank's accounting information systems, the penalty should be a

Warning	**Misdemeanor**	**Felony**
1	2	3

14. In your view, if someone were to destroy, copy, or alter any records in the bank's accounting information systems through direct manipulation, the penalty should be a

Warning	**Misdemeanor**	**Felony**
1	2	3

15. In your view, if someone were to destroy, copy, or alter any records in the bank's accounting information systems indirectly by introducing a computer virus, the penalty should be a

Warning	**Misdemeanor**	**Felony**
1	2	3