Appendix 3
The Results of Kruskal Wallis Test According to Bank Type

	Accidental entry of bad data by employees	Intentional entry of bad data by employees	Accidental destruction of data by employees	Intentional destruction of data by employees	Unauthorized access to the data and / or system by employees	Unauthorized access to the data and / or system by outsiders	Employees' sharing of passwords	Introduction (entry) of computer viruses to the system	Natural disaster	Human-made disasters
Chi-Square	1.709	5.662	1.949	.896	2.835	11.632	3.995	3.768	11.834	15.154
df	4	4	4	4	4	4	4	4	4	4
Asymp. Sig.	.789	.226	.745	.925	.586	.020	.407	.438	.019	.004

	Suppression or destruction of output	Creation of fictitious / incorrect output	Theft of data / information	Unauthorized copying of output	Unauthorized document visibility	Unauthorized printing and distribution of information	Prints are directed to people not entitled to receive	Sensitive doc. are handed to non- security cleared	Interception of data transmissions from remote locations
Chi-Square	3.089	8.361	9.306	1.984	1.644	1.111	6.436	3.145	1.986
df	4	4	4	4	4	4	4	4	4
Asymp. Sig.	.543	.079	.054	.739	.801	.892	.169	.534	.738

a Kruskal Wallis Test
b Grouping Variable: Bank Type

Appendix 4
The Results of Mann-Whitney Test According to Respondents Type

	Accidental entry of bad data by employees	Intentional entry of bad data by employees	Accidental destruction of data by employees	Intentional destruction of data by employees	Unauthorized access to data and / or system by employees	Unauthorized access to data and / or system by outsiders	Employees' sharing of passwords	Introduction of computer viruses to the system	Natural disaster
Mann-Whitney U	606.000	724.500	500.000	699.500	758.500	605.500	589.500	751.500	742.000
Wilcoxon W	1687.000	1285.500	1581.000	1260.500	1319.500	1686.500	1670.500	1832.500	1823.000
Z	-1.608	-.447	-2.891	-1.289	-.008	-2.048	-1.899	-.095	-.214
Asymp. Sig. (2-tailed)	.108	.655	.004	.197	.994	.041	.058	.924	.831

	Human- made disasters	Suppression or destruction of output	Creation of fictitious incorrect output	Theft of data / infor.	Unauthorized copying of output	Unauthorized document visibility	Unauthorized printing and distribution of information	Misdirection of Prints and distributed information	Sensitive documents handed to uncleared security personnel	Interception of data trans.
Mann-Whitney	650.000	731.500	673.500	628.000	716.500	655.000	647.500	668.500	741.000	717.000
Wilcoxon W	1731.000	1812.500	1754.500	1709.000	1797.500	1736.000	1728.500	1749.500	1822.000	1798.000
Z	-1.436	-.383	-1.543	-1.871	-.858	-1.608	-1.924	-1.079	-.390	-.630
Asymp. Sig. (2-tailed)	.151	.702	.123	.061	.391	.108	.054	.281	.697	.528

a Grouping Variable: Respondents Type

Appendix 2
The Frequencies of CAIS Security Threats

Accounting Information Systems Threats	Less than Once a year		Once a year to monthly		Once a month to weekly		Once a week to daily		more than once a day (frequently)	
	No.	%	No.	%	No.	%	No.	%	No.	%
1. Accidental entry of bad data by employees	4	5.1%	19	24.1%	35	44.3%	9	11.4%	12	15.2%
2. Intentional entry of bad data by employees	58	73.4%	20	25.3%	1	1.3%	0	0	0	0
3. Accidental destruction of data by employees	43	54.4%	28	35.4%	8	10.1%	0	0	0	0
4. Intentional destruction of data by employees	73	92.4%	6	7.6%	0	0	0	0	0	0
5. Unauthorized access to the data and / or system by employees	67	84.8%	12	15.2%	0	0	0	0	0	0
6. Unauthorized access to the data and / or system by outsiders (hackers)	60	75.9%	15	19.0%	2	2.5%	1	1.3%	1	1.3%
7. Employees' sharing of passwords is	45	57.0%	24	30.4%	5	6.3%	3	3.8%	2	2.5%
8. Introduction entry of computer viruses to the system is	57	72.2%	18	22.8%	4	5.1%	0	0	0	0
9. Natural disaster such as fire, flooding, loss of power, is	56	70.9%	21	26.6%	2	2.5%	0	0	0	0
10. Human- made disasters such as fire, loss of power	59	74.7%	19	24.1%	1	1.3%	0	0	0	0
11. Suppression or destruction of output is	62	78.5%	15	19.0%	1	1.3%	1	1.3%	0	0
12. Creation of fictitious / incorrect output is	70	88.6%	8	10.1%	1	1.3%	0	0	0	0
13. Theft of data / information	63	79.7%	16	20.3%	0	0	0	0	0	0
14. Unauthorized copying of output	72	91.1%	7	8.9%	0	0	0	0	0	0
15. Unauthorized document visibility by displaying on monitors or printed on paper is	66	83.5%	12	15.2%	1	1.3%	0	0	0	0
16. Printing and distribution of information by unauthorized persons.	69	87.3%	10	12.7%	0	0	0	0	0	0
17. Prints and distributed information are directed to people who are not entitled to receive	51	64.6%	26	32.9%	1	1.3%	1	1.3%	0	0
18. Sensitive documents are handed to non-security cleared personnel for shredding.	73	92.4%	5	6.3%	1	1.3%	0	0	0	0
19. Interception of data transmissions from remote locations	65	82.3%	13	16.5%	1	1.3%	0	0	0	0

Appendix 1

The Questionnaire

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

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

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

OECD (Organization for Economic Co-operation and Development) (1992), Guidelines for the Security of Information Systems, The Council of the OECD, 26 November.

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

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.

Rockwell, R. (1990), "The Advent of Computer Related Crimes", Secured Lender, (Jul /Aug), pp. 40 - 42

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

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

Schultz, E. E. (2002), "A Framework for Understanding and Predicting Insider Attacks", Computers & Security, (Vol. 21, Iss. 6), pp. 256 - 531.

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

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.

Smith, L. B. (1995), "On The New Beat", PC Week, (October30) (Vol. 12, No. 43), pp. E1-2.

Swann, J. (2004), "Always on the Case: Engaging your Staff in Bank Security", Community Banker, (March, Vol. 13, Iss. 3), pp. 44 - 47.

United States General Accounting Office (GAO) (2003), Information Security: Computer Controls over Key Treasury Internet Payment System, Report to Congressional Requesters, July.

Wackerly, D. D., W. Mendenhall and R. L. Scheaffer, (1996) Mathematical Statistics with Applications, Duxbury Press, Wadsworth Publishing Company, London.

Warren, M. J. (2002), Security practice: survey evidence from three countries, Logistics Information Manageme, (Vol. 15, Iss. 5/6), PP. 347-351.

Weingartner, A. and M. Burton (1991), "PC Security - Don't Be Caught Out", Computer Security Guide, pp. 33 - 35.

White, Gayle Webb and Sheila J Pearson (2001), "Controlling corporate e-mail, PC use and computer security"; Information Management & Computer Security, Vol. 9, Iss. 2/3; pp. 88-93.

Williams, P. (1995), "Safe, Secure And Up To Standard", Accountancy, p. 60.

Wood, C. C. and W. W. Banks (1993), "Human Error: An Overlooked but Significant Information Security Problem", Computers & Security, (Vol. 12, Iss. 1), pp. 51 - 60.

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.

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

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

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

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

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

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

KPMG (2000), Information Security Survey 2000, Executive Summary, April, KPMG, London.

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

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

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

Mclean, G. (2000), "The New Age of Bank Security", Canadian Banker, (Vol. 107, Iss. 4), pp. 14 - 19.

Mau, S. and J. Catlin (1993), "Systems Security in 90's", Interpreter, (January), pp. 8-9.

Meall, Lesley (1992), "Computer Crime: Foiling the Fraudsters", Accountancy, (November), pp. 56-57.

Melville S and W. Goddard (1996) Research Methodology: An Introduction for Science and Engineering Students, Juta and Co. Ltd, Kenwyn.

Miller, D. C. (1991) Handbook of Research Design and Social Measurement, (Fifth Edition), SAGE Publications, London.

Moss, N. (1996), "Banks at Mercy of Hackers", The European, October 10, N.335, p. 24.

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

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.

REFERENCES

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

Abu-Musa, A. A. (2003b), "Evaluating the Security Policies of Computerized Accounting Information Systems: An Evidence form Egyptian Banking Industry", The 28th International Conference of Statistics, Computer Science and Its Applications, Cairo, Egypt April 12-17.

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

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

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.

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

Corbitt, T. (1996), "Stop, Thief", Accountancy Age, (Feb), p. 20

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

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

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

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

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

Dickinson (1990), Statistical Analysis in Accounting and Finance, Philip Allan, London.

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

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

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

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

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

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

to receive it; and handling sensitive documents to non-security cleared personnel for shredding.

The results of the current study revealed that accidental entry of bad data by employees, accidental destruction of data by employees, introduction of computer viruses to the system, natural and man-made disasters, employees' sharing of passwords and misdirecting print-outs and distributing information to people not entitled to receive them are the most perceived significant security threats to CAIS in the EBS. Accordingly, it is recommended to strengthen security controls over the weak points in the Egyptian banking sector. From a practical standpoint, managers and practitioners alike stand to gain from the findings of this study. The results will enable managers and practitioners to better secure their CAIS and to promote information technology development for the success of businesses.

Further research could be undertaken to extend and improve the current study. The following aspects are suggested as extensions of the present research:

Firstly, the current research intended to investigate the security threats of CAIS in the EBS. More research is needed to have evidence from other developing countries. A comparative study could be carried out to investigate the significant differences between developing and developed countries regarding the CAIS security issues investigated.

Secondly, the current research was implemented in the banking sector. Further research could be carried out on other financial institutions, such as insurance companies. Evaluating the security of non-profit organizations, such as hospitals, general practitioners and national health services, could be another area for research where patients' health and personal information are under controls such as the UK's Data Protection Act. The telecommunication sector could be another fruitful area for empirical studies.

Thirdly, the current study focused on the banks' headquarters in the EBS. Further research could be extended to the bank branch level. It would be interesting to explore whether the branches face the same security threats and whether all the security controls implemented in banks' headquarters are replicated at the branch level.

Finally, the current research investigated the opinions of HoIAD, regarding the security threats of CAIS. It would also be possible to investigate the opinions of the external auditors regarding the materiality of those CAIS security threats.

(1999) employees might commit such computer crimes and steal from the business for which they work, the more common reasons being revenge, overwhelming personal debt, substance abuses and lack of internal controls. Business today is very competitive, and employees can often feel stressed. As a result, they have feelings of being overworked, underpaid and unappreciated. If employees are also struggling with serious personal problems, their motivation to commit fraud may be very high.

Although Egypt is not an active area for volcanoes or earthquakes and other similar natural disasters, the statistical results, surprisingly reported that natural (non- human) disasters is perceived as one of the significant security threats challenging CAIS in the EBS. Interviewing the respondents clarified such confusion, The respondents believe that non-human security threats of CAIS includes not only natural disasters (such as floods, earthquakes or failure of a power supply of the CAIS) but also technical security threats of using IT (such as technical failure of the system or hard disk failures) and the other IT technical facilities (such as software problems).

The statistical results of the study also showed no significant differences between different types of banks regarding the frequency of occurrence of CAIS security threats in the EBS, except for the unauthorized access to data and/or CAIS by outsiders (hackers). However, off-shore banks and banks which offer internet and phone banking services reported a higher perception of such security threat compared to other banks. The results tend to provide evidence of consistent perception of the significance of CAIS security threats across the EBS.

On the other hand, the results of the Mann-Whitney test (Appendix 4) reported significant differences between the opinions of the HoIAD and the HoCD, regarding the frequency of the following security threats in their banks: accidental entry of bad data by employees; accidental destruction of data by employees; employees sharing passwords and unauthorized printing and distribution of some data and information in the Egyptian banking sector. In all these cases, the HoIAD reported a greaer frequency of CAIS security threats compared to the HoCD. Consistent with the prior research (e.g. Hermanson et al., 2000; Coffin and Patilis, 2001; Wright and Wright, 2003; and Hunton et al 2005), it is observed that the HoCD focused more on unique risks and technical CAIS security threats compared to the HoIAD, who paid more attention to traditional risks and human security threats.

CONCLUSION AND RECOMMENDATIONS FOR FURTHER RESEARCH

The main objective of this paper was to investigate the significant security threats of CAIS, through their frequency of occurrence, in the EBS. A list of CAIS security threats was developed, based on previous studies (for example, Loch et al., 1992; Davis, 1996 and Henry, 1997) and available literature in this area. However, the following CAIS security threats were suggested and included in the security threats list to be investigated for the first time: man- made disasters such as fire, loss of power; suppression or destruction of output; creation of fictitious / incorrect output; theft of data / information; unauthorized copying of output; unauthorized visibility of documents; unauthorized printing and distribution of information; directing print-outs and distributing information to people who are not entitled

19. Interception of Data Transmissions

It is observed that the majority of respondents (82.3 percent) considered that the interception of data transmission very rarely occurred in their banks. 16.5 percent of respondents reported that it occurred once a year to monthly; only one respondent (1.3 percent) believed that interception of data transmissions occurred once a month to weekly. The above results suggest that the frequency of this threat is quite low in the EBS.

DISCUSSION OF THE RESULTS

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

The results of the current study also revealed that accidental entry of bad data by employees, accidental destruction of data by employees, introduction of computer viruses to the system, man-made disasters, employees' sharing of passwords, and misdirecting prints and distributing information to people not entitled to receive them, are reported as the most perceived significant security threats to CAIS in the EBS. The results provide further evidence that the big security headaches are now perceived to come from within, not outside. This result is consistent with Loch et al., 1992; OECD, 1992; Davis, 1996; Weingartner and Burton, 1991; Jenkins et al., 1992; and Henry, 1997, suggests that the organization's own employees are potentially its own worst enemies, posing the most serious risk to security. Anderson (1994) confirmed that many thefts in banks, as well as many frauds in other industries, are carried out by employees who have inside knowledge and access. It is reported that British banks dismiss about one percent of their staff every year for disciplinary reasons. Many of these sackings are for petty thefts by tellers, and many ATM related thefts go undetected because of the banks' policy of denying that they are even possible.

Intentional acts such as entry of bad data, destruction of data, introduction of computer viruses, and man made disasters, generally fall into the designation of computer crime. These crimes might be acts of sabotage intended to destroy the CAIS components or acts of computer fraud where the intent is to steal money, data, computer time and/or services. They would also include manipulative activities such as deleting or altering records and files to remove damaging information or create false information. However, according to the results of the current study, it seems that intentional entry of bad data and destruction of data by employees rarely happen in the EBS. The results of the survey were not consistent with the researcher's expectations and observations related to the increasing number of the reported computer crimes in the EBS. However, there are many possible reasons for committing computer crime such as embezzlement and computer fraud. According to Haugen and Selin

14. Unauthorized Copying of Output

The results revealed that a vast majority of the respondents (91.1 percent) reported that unauthorized copying of output was rare, since it occurred less than once a year. However, a minority (8.9 percent) believed that it occurred once a year to monthly. The result provides an indicator of the low occurrence frequency of unauthorized copying of output in the EBS.

15. Unauthorized Document Visibility

The statistics revealed that the great majority of respondents (83.5 percent) believed that unauthorized document visibility, by displaying it on monitors or printed on paper, was very rare, as it occurred less than once a year, while the minority (15.2 percent) believed that it occurred once a year to monthly, which is still considered as a very low level of occurrence. Only one respondent believed that it happened once a month to weekly in his bank. According to the above result, unauthorized document visibility seems to be a very low level threat in the EBS.

16. Unauthorized Printing and Distribution of Data / Information

The result shows that the majority of respondents (87.3 percent) considered the frequency of unauthorized printing and distribution of information to be extremely low in their banks (less than once a year). Only 12.7 percent of respondents believed that it happened in their banks between once a year to monthly. The results provide evidence of the low frequency of unauthorized printing and distribution of information in the EBS.

17. Directing Prints and Distributed Information to People Not Entitled To Receive

The statistics revealed that some two-thirds of respondents (64.6 percent) indicated that this threat was very rarely encountered in their banks (less than once a year). However, approximately 33 percent of the respondents believed that it happened once a year to monthly. On the other hand, only two respondents (2.6 percent) mentioned that it occurred either once a year to monthly or once a week to daily.

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

The vast majority of respondents (92.4 percent) reported that handing sensitive documents to non-security-cleared personnel for shredding very rarely occurred in their banks. Five respondents (6.3 percent) believed that this might happen once a year to monthly; while only one respondent believed that it occurred once a month to weekly. These findings strongly support the view that the frequency of handing sensitive documents to non-security cleared personnel for shredding is very low in the EBS.

The results showed that the majority of respondents (approximately 71 percent) confirm the rarity of natural disasters in the EBS. Such natural disasters as earthquakes or loss of electricity occasionally happened, but less than once every several years. Moreover, floods and wind disasters very rarely occur in Egypt. 26.6 percent of the respondents believed that they could happen once a year to monthly, while only 2.5 percent of respondents believed that natural disasters might occur once a month to weekly.

10. Disasters of Human Origin

Man-made disasters include those disasters, such as fires, floods and explosions. However, man-made disasters could occur as a result of intentional or accidental actions. Many intentional acts are classified as crimes, such as fraud, theft, embezzlement, extortion, larceny and mischief. The results also revealed that approximately three-quarters of respondents considered that a man-made disaster is a very rare event in their banks, with an occurrence of less than once a year. 24 percent of respondents reported that this threat was rarely encountered in their banks. Only one respondent believed that it happened once a month to weekly. The information above provides an indicator on the low reported frequency of man-made disasters in the EBS.

11. Suppression or Destruction of Output

The research findings show that the majority of respondents (78.5 percent) believed that suppression or destruction of their banks' output occurred less than once a year. A further 19 percent of the respondents confirmed the occurrence of that security threat to be rare. Only two respondents, representing 2.6 percent of the total, believed that suppression or destruction of their banks' output occurred more than once a week to monthly. This finding provides support for the rare frequency of the suppression or destruction of banks' output in the EBS.

12. Creation of Fictitious / Incorrect Output

The findings reveal that the great majority of respondents (88.6 percent) believed that creation of fictitious / incorrect output rarely happened, occurring less than once a year. A minority of respondents (10 percent) believed that creation of fictitious / incorrect output might occur once a year to monthly, which can still be considered as a very low level of occurrence. According to the above result, the creation of fictitious / incorrect output seems to be a very low level security threat in the EBS.

13. Theft of Data / Information

The great majority of the respondents (approximately 80 percent) indicated that theft of data / information was rare in their banks, since it might occur less than once a year. However, 20 percent of the respondents believed that it could happen once a year to monthly. According to the above result, theft of data / information seems to be an infrequent security threat in the EBS.

6. Unauthorized Access to the Data and / or Systems by Outsiders

The majority of the respondents (approximately 76 percent) indicated that unauthorized access to the data and / or systems by outsiders (hackers) rarely happened in their banks: less than once a year. However, 19 percent of the respondents believed that it could happen once a year to monthly. One possible interpretation of this result is that electronic banking services (such as phone banking; electronic fund transfer and corporate-banking) is not widespread and accepted in the EBS. On the other hand, two respondents, representing 2.5 percent of responses believed that unauthorized access to the data and / or systems by outsiders (hackers) happened once a month to weekly, one respondent indicated that it occurred once a week to daily, while another respondent affirmed that it happened more frequently in his bank.

7. Employees' Sharing of Passwords

The results show that slightly more than half of respondents (57 percent) believed that sharing of passwords seldom occurred in their banks. However, 30.4 percent of respondents reported that it rarely happened: from once a year to monthly. Five respondents (6.3 percent) believed that sharing of passwords occurred once a month to weekly; three respondents (3.8 percent) believed it happened once a week to daily; and two respondents (2.5 percent) believed this happened more than once a day or more frequently in their banks. The above results tend to suggest that the employees' sharing of passwords is considered as frequent security threats in the EBS.

8. Introduction (Entry) of Computer Viruses to the System

Regarding to introduction of computer viruses to the system, the results show that the majority (72.2 percent) reported that the introduction of computer viruses seldom occurred: its probability was less than once a year. Approximately 23 percent of the respondents believed that it happens once a year to monthly; while only 5 percent of respondents believed it occurred once a month to weekly. From the finding above, it is observed that the reported frequency of the introduction of computer viruses is quite low in the EBS. The possible reason for this could be that the majority of banks use mainframe computer systems, booting the original programs and software packages, and almost all use disk-less computers.

9. Natural Disasters

In relation to the frequency of occurrence of natural disasters in the EBS, respondents were asked to indicate its occurrence in their banks. According to Parker (1976) "Natural disasters caused by fire, water, wind, power outages, lightning, and earthquakes could cause significant disruption (or even destruction) of computer facilities, or at least crucial parts of computer facilities" (p. 14).

2. Intentional Entry of Bad Data by Employees

The statistics show that the majority of respondents (73.4 percent) expressed belief that it happened very rarely in their banks, being likely to occur even less than once a year. They considered it as a crime and a kind of computer fraud; therefore, whoever committed such a crime should be prosecuted. 25.3 percent of the respondents believed that intentional entry of incorrect data rarely occurred in their banks, happening once a year to monthly. They too, considered that legal action should be taken against whoever commits it. Only one respondent believed that intentional entry of incorrect data by employees happened relatively frequently in his bank. He believed it might occur once a month to weekly, due to the large, scattered number of the bank's branches and, moreover, the inadequacy of implemented controls.

3. Accidental Destruction of Data by Employees

The results revealed that slightly more than half of the respondents (54.4 percent) believed that the frequency of accidental destruction of banks' data as a result of employees' errors or mistakes was less than once a year. 35.4 percent of the respondents indicated that that could happen once a year to monthly and only 10 percent of respondents believed that accidental destruction of data might happen once a month to weekly. When the respondents were interviewed, one of them mentioned that it would not be surprising if such destruction occurred, bearing in mind that the bank has several hundred branches and that a lot of new employees are hired every year who need more training. It was seen as an inconsequential threat, since data could be easily recovered through the bank's excellent back up system.

4. Intentional Destruction of Data by Employees

The results show that the great majority of the respondents (92.4 percent) believed that this very rarely occurred in their banks, since it might happen less than once a year. However, a minority of the respondents (7.6 percent) mentioned that it could occasionally, but not frequently, happen, triggered by some embezzlement by employees. Thus, it is observed that the frequency of intentional destruction seems to be quite low in the EBS.

5. Unauthorized Access to the Data and / or System by Employees

The majority of the respondents (85 percent) claimed that unauthorized access to their banks accounting systems rarely happened. They reported that it might occur less than once a year, due to secure implemented password systems. A minority of respondents (15 percent) believed that unauthorized access to their banks' accounting systems by internal employees might occur once a year to monthly, which can still be considered as a very low level of occurrence. According to the above result, unauthorized access to the banks' accounting systems / data by employee seems to be an infrequent security threat in the EBS.

* Most parametric tests need large samples to be used efficiently. Parametric tests typically require that the sample should have more than 50 observations. A non-parametric test does not require a certain size of sample;

* Parametric test assumptions assume that observations are normally distributed. Because of the small number of Egyptian banks' headquarters, the normal distribution of the data cannot be guaranteed. Non-parametric tests do not require any special distribution of the research population, since these tests are "distribution free". Thus they are more suitable for the current study;

* Parametric tests require collected data to be numerical. Thus they are more suitable for interval and ratio data. Since most of the data collected in the current study is not truly numerical, parametric tests would not be the appropriate. Non-parametric tests are more suitable, because they can deal with nominal, ordinal, categorical, and scale ranked data (See: Dickinson, 1990; Miller, 1991; Hessler, 1992; Melville and Goddard, 1996; Wackerly et al., 1996; and Abu-Musa 2003b).

THE RESULTS

The results of the current study revealed that many of the surveyed Egyptian banks suffered financial security losses due to disgruntled or dishonest internal (employees) and external (hackers) actions. The financial security losses ranged from 50,000 to 250 millions Egyptian pounds. However, the reporting of losses might be a sensitive and potentially unreliable data item collected in the current study, since many banks were reluctant to report their actual losses. It is observed that even in cases where computer-related fraud were discovered and the perpetrator identified, banks were reluctant to involve the police. Banks believe that would negatively affect their reputation and indicate a weakness in their CAIS to shareholders, potential customers and competitors. The results obtained from this study were consistent with the results of other previous studies in this area (see: Doost, 1990; Rockwell, 1990; Meall, 1992; Feeney, 1993; EDPACS, 1992; Mau and Catlin, 1993; Corbitt, 1996; Moss, 1996; and KPMG, 2000). The main findings relating to the important perceived security threats challenging CAIS in the EBS, are presented in the following sections.

1. Accidental Entry of Bad Data by Employees

Respondents were asked to indicate the frequency of accidental entry of bad data by employees, by ticking one of five available choices. The results revealed that the majority of respondents (44.1 percent) believed that accidental entry of bad data by employees happened between once a month and weekly; 24 percent of the respondents believed this might happen from once a year to monthly; 5 percent of the respondents believed that accidental entry of bad data by employees very rarely happened in their banks, since it occurred less than once a year. On the other hand, 11.4 percent of the respondents claimed the occurrence of accidental entry of incorrect data, between once a week to daily; while 15.2 percent of them believed that it happened daily or more frequently in their banks. Many respondents qualified their report, stating that no harm is done as long as such mistakes are discovered and corrected in the final or half-day audit reports.

(Table 1: The Response Rate of the Headquarters Sample)

The Bank Type	Total N. of banks		Responding Banks				Respondents type	
	Total N.	Net N.	Initial Rate		Revised Rate		Computer Dept.	Internal Audit Dept.
Commercial Public Banks	4	4	2	50%	2	50%	2	1
Specialized Public Banks	4	3*	2	50%	2	66.7%	2	2
Commercial Private Banks	23	22**	19	82.7%	19	86.5%	19	17
Joint Venture Banks	15	15	14	93.4%	14	93.4%	14	5
Branch of Foreign Banks	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 banks were merged into one bank
** One bank was too distant to visit
*** 3 banks were under liquidation; 2 banks had non - Computerized systems; and in one bank the researcher was not able to meet the target respondents.

The response rate in each category implies that each category is represented in the sample. 93.3 percent of Egypt's joint venture banks and 82.7 percent of the commercial private banks participated in this survey. Moreover, 45 percent of the local headquarters of foreign banks, 50 percent of the commercial public banks and 66.7 percent of the specialized public banks were involved in the research sample and data analysis.

Moreover, the researcher carried out an unstructured interview to explore the respondents' opinions regarding the relative importance of CAIS security threats; the financial security losses in the last twelve months due to internal and external actions and the adequacy of implemented security controls to prevent, detect and correct such security breaches in their banks.

The collected data has been processed and analyzed using the statistical package for social sciences (SPSS) version 12. Descriptive statistics (such as frequencies and percentages) of the collected data had been carried out to recognize and understand the main characteristics of the research variables. In addition, non-parametric tests (such as Kruskal-Wallis test; and Mann-Whitney test) had been carried out to examine whether there are any significant differences among different types of banks as well as different respondents groups regarding their perceived security threats of CAIS in the EBS.

Dickinson (1990) reported that non-parametric tests are designed to deal with ordinal data and categorical data, whereas parametric tests can be used only when the data are strictly measurable on numerical scales (p. 131). Miller (1991) also confirmed that "nominal and ordinal scales require nonparametric tests; only interval and ratio scales may permit use of parametric tests" (p. 245).

Therefore, it is argued that non-parametric tests - rather than parametric tests - are the most suitable statistical tests for analyzing data collected in the current study, due to the following reasons:

HYPOTHESES

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

H01: There are significant differences between different types of banks regarding the frequency of occurrence of CAIS security threats in the EBS.

H11: There are no significant differences among different types of banks regarding the frequency of occurrence of CAIS security threats in the EBS.

H02: There are significant differences in the opinions of the HoCDs and the HoIADs regarding the frequency of occurrence of CAIS security threats in the EBS.

H12: There are no significant differences in the opinions of the HoCDs and the HoIADs regarding the frequency of occurrence of CAIS security threats in the EBS.

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 EBS regarding the significant security threats challenging their CAIS. The respondents were asked to indicate the frequency of occurrence of each security threat by ticking one among five available choices (less than once a year; once a year to monthly; once a month to weekly; one a week to daily; and more than once a day or more frequently).

The questionnaire was piloted and pre-tested on selected members of PhD students; academic faculty and accounting practitioners. The questionnaire was also piloted on a selected sample of Egyptian banks. Comments and suggestions were considered in developing and revising the final questionnaire. Reliability test has been carried out on the questionnaire using the Alpha Cronbach model, to explore its internal consistency, based on the average inter-item correlation. The result of the reliability test shows that the questionnaire design is highly reliable regarding the frequency of occurrence of security threats (Alpha = 0.7685).

The entire population (sixty-six banks' headquarters) of the Egyptian banking sector has been surveyed in the current study. Seventy-nine completed and usable questionnaires were collected from forty-six different banks' headquarters. Forty- six of these questionnaires were completed by the heads of computer departments, and thirty-three questionnaires were filled by the heads of internal audit departments. The response rate of the computers departments (after excluding merged, liquidated, too distant, and non computerized banks) was 79.3%, whilst the response rate was 56.9% from the internal audit departments. Both can be considered high response rates. The initial and revised banks' response rates are illustrated in table (1):

In the current study, security threats and controls have been carefully distinguished. A selected number of precise security threats to CAIS are derived from previous studies (Loch et al., 1992; Davis, 1996 and 1997; FFIEC, 1996; and Henry, 1997). In addition, the following CAIS security threats are included in the proposed security list to be empirically examined for the first time:

* Man- made disasters such as fire, and loss of power;
* Suppression or destruction of output ;
* Creation of fictitious / incorrect output;
* Theft of data / information;
* Unauthorized copying of output;
* Unauthorized visibility of documents;
* Unauthorized printing and distribution of information;
* Directing prints and distributing information to people who are not entitled to receive it; and
* Giving sensitive documents to non-security cleared personnel for shredding.

It is also observed that almost all the previous studies in CAIS security threats research area have been implemented in developed countries; and according to the author's knowledge no empirical research has examined CAIS security threats in developing countries. It is believed that conducting the current study in a developing country, Egypt, can thus yield significant results. The research strategy was to conduct an intensive empirical study, to investigate the security threats of CAIS in one sector, rather than spread the effort over a wide range of different sectors. EBS was selected to accomplish and implement the empirical work for the following reasons:

1. The banking sector is the most organized sector, compared to other sectors;

2. The banking sector is one of the leading sectors, which affects the economic and development process in Egypt;

3. Most banks have computerized accounting information systems, which is considered a relevant environment to implement the current study;

4. The daily operations of banks depend to a great extent on the reliability, accuracy, availability, and integrity of information, which are the main targets of CAIS security;

5. Banks as a financial sector, usually put information security at higher priority, and pay considerable attention to the security issues, compared with other sectors;

6. Selecting one sector (the banking sector) rather than different sectors, offers some advantages to the research, since respondents in the same sector are working in a similar environment and they have similar skills and backgrounds, which may promote standadisation of the data.

The United States General Accounting Office (GAO) (2003) performed a review of 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 systems protection. The results of the GAO's review (2003) revealed that although FMS and the Federal Reserve had 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 to promptly address new security threats and risks as they emerge to CAIS, were recommended.

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

THE IMPORTANCE OF THE RESEARCH

Reviewing the literature, it is observed that many of the previous studies (e.g., Loch et al. 1992; Davis, 1997; Ryan and Bordoloi, 1997; and Henry, 1997) did not always distinguish clearly between security threats and the inadequacy of security controls. Previous studies treated some inadequate or ineffective security controls as security threats. For example, the lack or inadequacy of some security controls (such as inadequate control over media [disks and tapes]; poor control over manual handling on input / output; poor segregation of information systems duties; poor segregation of accounting duties; inadequate control over storage media; inadequate audit trail, the inadequacy or non-existence log-on procedures, losses due to inadequate backups or log files, uncontrolled read and / or update access, uncontrolled user privilege, and weak / ineffective or inadequate physical controls) were considered as security threats. This is confusion: weak policing does not itself create the crime.

However, Ryan and Bordoloi (1997) acknowledged that some of the items might not be considered security threats in the strict sense of the term; nevertheless, they argued, they might matter very much to the continued existence of the organization. The researchers therefore included them in their survey and reported them as important to good information technology management and practice (p. 139).

White and Pearson (2001) surveyed over two hundred US companies to investigate the security controls of 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 corporations began to use computer technology before implementing appropriate safeguards and the majority of companys' safeguards required updating.

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

* In Australia, poor levels of computer security were found among Australian organizations. Many of the security problems were identified due to poor security procedures being implemented. The results also indicated that 45 percent of organizations did not budget for computer security.

* In UK, 42 percent of organizations did not have an information security policy. The findings also revealed that 49 per cent of organizations listed budget constraints as being an issue in implementing computer security.

* While in USA, theft of information and financial fraud caused the most financial damage. However, differences in the levels of CAIS abuses carried out by internal and external individuals were not significant. The paper suggested that USA security practices seem to be more effective than those of Australia or the UK.

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

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

Henry (1997) conducted a survey to determine the nature of the accounting systems and security in use. The results of Henry's survey indicated that 80.3 percent of companies, backed-up their accounting systems. 74.4 percent of companies secured their accounting system with passwords, but only 42.7 percent utilized protection from viruses. Physical security and authorization for changes to the system were employed by less than 40 percent of the respondents. The survey results also showed that only 15 companies used encryption for their accounting data, which was a surprising result, considering the number of companies utilizing some form of communication hardware. Almost 45 percent of the sample underwent some sort of audit of CAIS data.

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

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

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

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

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

objectives of previous studies under this category, have been to list the security threats that might threaten computerized information systems in an organization; to explore the significance of such perceived security threats in the real world and to investigate their occurrence and potential losses in different organizations.

One of the most important studies in this area was carried out by Loch et al. (1992). The researchers conducted a survey to explore the perception of Management Information Systems Executives regarding the security threats in microcomputer, mainframe computer, and network environments. The researchers developed a list of twelve security threats, which were empirically examined. The results indicated that natural disasters; employee accidental actions (entry of bad data and destruction of data); inadequate control over media; and unauthorized access to CAIS by hackers, were ranked among the top security threats. These results confirmed the experts' claims that the greatest threats come from inside organizations.

Since accounting information system security has become one of the major concerns for information system auditor, Davis (1996) tried to discover the current status of the security issue in practice. Davis conducted a survey using the questionnaire, "Threats to Accounting Information Systems Security Survey" which was adapted from Loch et al. (1992), in replication of their work. The results of Davis' survey (1996) indicated that information systems auditors recognized that different computing environments have different relative levels of security risks.

The results of Davis' (1996) study also reported that employees' accidental entry of "bad" data and the accidental destruction of data, as well as the introduction of computer viruses, were considered to be the three top threats in a microcomputer environment. However, unauthorized access to data and/or systems by employees, accidental entry of "bad" data by employees and poor segregation of information system duties, were rated as the major threats to the minicomputer environment. Concerning the mainframe computer environment, accidental entry of "bad" data by employees, natural disaster, and unauthorized access to data and/or systems by employees, were perceived as the main threats, while unauthorized access to data and/or systems by both outsiders (hackers) and insiders (employees), and technology advances faster than control practices were said to be the most important threats in network computer environment.

Recently, client / server computing became a serious alternative to mainframe computing in many organizations. Although the client / server computing system offers some benefits, it also exposes the computing environment to additional risks: the flexibility that makes it attractive can also make it more vulnerable to security threats. Ryan and Bordoloi (1997) explored how companies moving from a mainframe to a client / server environment evaluated and took security measures to protect against potential security threats. The results of Ryan and Bordoloi's (1997) study revealed that the most significant security threats were: accidental destruction of data by employees; accidental entry of erroneous data by employees; intentional destruction of data by employees; intentional entry of erroneous data by employees; loss due to inadequate backups or log files; natural disaster: fire, flood, loss of power, etc., and single point of failure.

security problems. Therefore, the more informed users are, the more likely they are to accept the policies". Again, Wood and Banks (1993) stated that human error is one of the major and most serious threats to information security that is often ignored or dismissed with statements such as "it's inevitable" or "there is not much we can do about it". This type of thinking runs counter to reality, since studies have shown that, of all systems threats, human error has the highest probability of occurring. The previous studies also indicated that, with the right professional assistance, human errors could be easily corrected or significantly reduced. According to Haugen and Selin (1999) unintentional acts, while costly at times, could be corrected or avoided through training and supervision.

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". Accordingly, 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 potartial security risks. Developing information security policy and enhancing employees' awareness, regarding information security are very important issues.

The objective of this paper is to investigate the perceived security threats of CAIS in developing countries. The entire population of the Egyptian banking Sector (EBS) has been surveyed to investigate the significant differences among different respondents groups as well as types of banks, regarding the perceived security threats of CAIS using a proposed security threats checklist.

The current study is a trial to investigate the following research questions:

1. What are the most important perceived security threats challenging CAIS in the EBS?
2. Are there significant differences among different types of banks, regarding their perception of CAIS security threats in the EBS?
3. Are there significant differences between the opinions of the heads of internal audit departments (HoIAD) and the heads of computer departments (HoCD) regarding the perceived security threats of CAIS in the EBS?

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

LITERATURE REVIEW

Reviewing the literature concerned with evaluating the security of computerized information systems reveals the paucity of available studies in that particular area of research. One reason is that the security of CAIS is a relatively new research area. The main

INTRODUCTION

The rapid change in computer technology, the widespread use of user-friendly systems and the great desire of organizations to acquire and implement up-to-date Computerized systems and software, have made computers much easier to use and enabled accounting tasks to be accomplished much faster and more accurately than before. On the other hand, this advanced technology has also created significant risks relating to the security and integrity of computerized accounting information systems (CAIS). The technology, in many cases, has developed faster than the advancement in control practices and has not been combined with similar development of employees' knowledge, skills, awareness, and compliance (Abu-Musa, 2003a). Davis (1996) mentioned that great changes in computer technology are occurring with greater frequency than ever before, and many of these changes are being adopted into organizations' accounting information systems. These technological advancements have created new security threats to CAIS.

Computerized systems are vulnerable to many threats that can inflict various types of damage resulting in significant losses. This damage can range from errors harming database integrity to fires destroying entire computer centers. Losses can stem, for example, from the actions of supposedly trusted employees defrauding a system, from outside hackers, or from careless data entry clerks. Precision in estimating computer security-related losses is not possible because many losses are never discovered, and others are "swept under the carpet" to avoid unfavorable publicity (National Institute of Standards and Technology, 1995).

The security threats of CAIS and electronic information could be in the form of: loss of information privacy; theft of information; unauthorized use of information; fraudulent use of information and computers; loss of information integrity as a result of unauthorized intentional change or manipulation of data; or loss of computing services due to unauthorized or intentionally malicious actions (Schweitzer, 1987). Haugen and Selin (1999) classified the common types of computer-based fraud under the following six categories: altering input; theft of computer time; software piracy; altering or stealing data files; theft or misuse of computer output; and unauthorized access to systems or networks.

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

Smith (1995) confirmed that "creating a secure environment is complicated by the fact that workers must support security efforts for them to be effective, but it is often employees that pose the greatest threat to security. Most workers, however, are not actively trying to breach security. Often, careless mistakes and indiscriminate access to information are at the root of

---

[19] Dr Ahmad A. Abu-Musa is an Assistant Professor at the Department of Accounting & Managing Information Systems, College of Industrial Management, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia.

106 The Arab Journal of Accounting
Vol. 9 N0. 1
May 2006
PP. 106-129

A Study of the Perceived Security Threats of Computerized Accounting Information Systems: The Case of Egyptian Banking Sector

Ahmad A. Abu-Musa
King Fahd University of Petroleum and Minerals

ABSTRACT

The objective of this paper is to investigate the perceived security threats of computerized accounting information systems (CAIS) in developing countries. The entire population of the Egyptian banking sector (EBS) has been surveyed to achieve the purpose of the paper. The differences between the respondents' opinions as well as bank types regarding the perceived security threats have been identified and investigated in the context of the EBS. The results revealed that accidental entry of bad data by employees, accidental destruction of data by employees, introduction of computer viruses to the system, natural and man-made disasters, employees' sharing of passwords and misdirecting prints and distributing information to people not entitled to receive them, are perceived as the most important security threats to CAIS in the EBS. In all these cases, the heads of internal audit departments reported increased frequencies of CAIS security threats, compared with the heads of computer departments.

Key Words: Perceived Security Threats; Information Technology; Accounting Information Systems; Egyptian Banking Sector; Empirical Survey