JOURNAL OF INFORMATION SYSTEMS
Vol. 20, No. 1
Spring 2006
pp. 187–203

Perceived Security Threats of Computerized Accounting Information Systems in the Egyptian Banking Industry

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

ABSTRACT: This paper investigates the perceived security threats to computerized accounting information systems (CAIS) in the Egyptian banking industry (EBI) by surveying the entire population of the EBI. Differences between the respondents' opinions regarding the perceived security threats have been identified and investigated in the context of the EBI. The results of the study reveal that accidental entry of bad data by employees, accidental destruction of data by employees, introduction of computer viruses to the system, natural and human-made disasters, employees' sharing of passwords, and misdirecting prints and distributing information to unauthorized people are the most significant perceived security threats to CAIS in the EBI. In all cases, the heads of internal audit departments reported higher occurrence frequencies of CAIS security threats compared to the heads of computer departments.

Keywords: computer security threats; accounting information systems; Egyptian banking industry.

I. INTRODUCTION

Advanced technology has created significant risks related to ensuring the security and integrity of computerized accounting information systems (CAIS). The technology, in many cases, has been developed faster than advances in control practices and employees' knowledge, skills, awareness, and compliance (Abu-Musa 2003a).

According to the National Institute of Standards and Technology (1995) ''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.''

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

I thank the reviewers of the *Journal of Information Systems* for their constructive suggestions. I also would like to thank Professor Brad Tuttle, the current editor, and Professor Dan Stone, the former editor, for their superb, thorough editorial support and guidance.

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 likely 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 to CAIS in the Egyptian banking industry (EBI). The entire population of the EBI has been surveyed to investigate the significant differences among different bank types as well as respondent groups regarding their perceived security threats to CAIS. The security threats checklist used in the study is based on the available literature and the previous empirical studies in this area. It includes many security threats which are empirically tested here for the first time. This research attempts to answer the following questions:

(1) What are the most important perceived security threats challenging CAIS in the EBI?
(2) Are there significant differences among different bank types regarding their perception of CAIS security threats in the EBI?
(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 to CAIS in the EBI?

The remainder of this paper is organized as follows. The next section presents the literature review and previous studies related to the perceived security threats of CAIS. Section III highlights the importance of the current research; and Section IV introduces the research methodology. Section V presents the major empirical results of the current research; this is followed by a discussion of the research findings in Section VI. The final section of the paper provides the study's major conclusions and recommendations for further research.

II. LITERATURE REVIEW

Reviewing the literature concerned with evaluating the security threats to CAIS reveals the paucity of available studies in this particular area of research. One reason is that the security of CAIS is a relatively new research area. The main objectives of previous studies under this category have been to list the security threats that might threaten computerized information systems in an organization; to explore the significance of such perceived security threats; 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 surveyed the perceptions 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 to be empirically examined in that study. The results of the study indicate that natural disasters, employee accidental actions (entry of bad data and destruction of data), inadequate control over media, and unauthorized access to systems by hackers were ranked among the top security threats.

Davis (1996) attempted to discover the current status of IS security practice using the questionnaire developed by Loch et al. (1992), in replication of their work. The results of Davis's (1996) survey indicate that information systems auditors recognized that different computing environments have different relative levels of security risks. The results of the

study also show 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 security 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 midrange computing environment. Concerning the mainframe computer environment, accidental entry of ''bad'' data by employees, natural disaster, and unauthorized access to data and/or system by employees were perceived as the main threats. Unauthorized access to data and/or systems by both outsiders (hackers) and insiders (employees), and technology advancing faster than control practices were identified to be the most important threats in network computer environments.

Ryan and Bordoloi's (1997) research explored how companies moving from a mainframe to a client/server environment evaluated and took security measures to protect against potential security threats. The results of Ryan and Bordoloi's (1997) study reveal 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 including fire, flood, loss of power, etc., and single point of failure.

Hood and Yang (1998) studied the security of banking information systems in China. The survey results reveal that all respondents believe that management was aware of security issues but none believed that their banks had taken enough action to reduce the risks and losses due to the lack of financial and human resources. Furthermore, all four banks surveyed claimed to have a security policy, but only in one was it formally stated. Human security threats were perceived as the most important security threats in the Chinese banking industry, especially malicious attack from outsiders. These differences suggest that developing countries perceive security differently.

Reviewing the nature of security breaches that have taken place in different parts of the world, Dhillon (1999) argues that many of the security losses resulting from computer-related fraud could be avoided if organizations adopt a more pragmatic approach in dealing with such incidents. The results of Dhillon's (1999) study suggest that implementing controls, as identified in a security policy, would indeed deter computer misuse. Adopting a balanced approach of security controls which place equal emphasis on technical, formal, and informal interventions to CAIS would prevent committing computer fraud.

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. The results of the study reveal that internal auditors focus primarily on traditional IT risks and controls, such as safeguarding IT assets, application processing, and data integrity, privacy, and security.

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

White and Pearson (2001) surveyed over 200 U.S. companies to investigate the security controls related to the personal use of computers, controlling email accounts, and securing company data. The results of the study reinforce the need for better security control in the

majority of surveyed companies. The results also reveal that many corporations began to use computer technology before implementing appropriate safeguards; and in the majority of companies safeguards continue to be lacking.

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

- In Australia, poor levels of computer security were found among Australian organizations. Many of the security problems were identified as implementation of poor security procedures. The results also indicate that 45 percent of organizations do not budget for computer security.
- In the U.K., 42 percent of organizations did not have an information security policy. The findings also reveal that 49 percent of the organizations listed budget constraints as being an issue in implementing computer security.
- In the U.S., theft of information and financial fraud causes the most financial damage. However, differences in the levels of CAIS abuses carried out by internal and external individuals were not significant. The paper suggests that U.S. security practices seem to be more effective than those of Australia or the U.K.

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 show that the potential for financial statement errors and business risks is intensified as a result of the lack of proper user training. The findings also show that ongoing risks differ across applications and across vendor packages. Finally, the results suggest that major firms use process audit techniques, as opposed to validation testing (i.e., they do not rely on tests of output), when hired to provide assurance on the risks for an ERP system.

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

The United States General Accounting Office (GAO) (2003) performed a review at the Financial Management Service (FMS) during the period from October 2002 to June 2003 to investigate whether FMS: (1) conducted a comprehensive security risk assessment and (2) documented and implemented appropriate security measures and controls for the system's protection. The results of the GAO (2003) review 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 and to promptly address new security threats and risks as they emerge to CAIS were highly recommended.

It is also observed that almost all the previous studies in the information security research area have been implemented in developed countries and none have investigated

CAIS security issues in developing countries. It is believed that conducting this research in one developing country, Egypt, can thus yield fruitful results.

III. THE IMPORTANCE OF THE CURRENT RESEARCH

Reviewing the literature, it is observed that most of the previous studies (e.g., Loch et al. 1992; Davis 1997; Ryan and Bordoloi 1997) do not clearly distinguish between security threats (i.e., possible negative events) and security weaknesses (i.e., inadequate security controls). For example, the 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, and poor segregation of accounting duties are treated as security threats. Further, inadequate control over storage media, inadequate audit trial, inadequate or nonexistent log-on procedures, loss due to inadequate backups or log files, uncontrolled read, and/or update access, uncontrolled user privilege, and weak/ineffective or inadequate physical controls are also considered as security threats.

In this research, security threats and controls have been carefully distinguished. A selected number of precise security threats to CAIS were derived from previous studies (e.g., Loch et al. 1992; Davis 1996, 1997; FFIEC 1996; Ryan and Bordoloi 1997) and other available literature in this area. Moreover, some additional security threats are investigated for the first time in the current research (for example, threats numbers 10 through 19 in the Appendix). The additional security threats, mainly related to the output of CAIS, have been overlooked in the previous studies.

The present research strategy was to conduct an intensive investigation into the security threats of CAIS in one industry, rather than spread the effort over a wide range of different industries. Selecting one industry (the banking industry) rather than different industries offers some advantages because respondents in the same industry are working in similar environments and they have similar skills and backgrounds, which may promote homogeneity of the data. The EBI was selected for two important reasons. First, Egypt represents a developing economy in which the banking industry is one of the most advanced in terms of CAIS and key to its economic infrastructure. This represents a similar pattern to other developing economies (e.g., China). Second, the daily operations of a bank depend to a great extent on the reliability, accuracy, availability, and integrity of information, which are the main targets of the security of CAIS.

The approach used in the current survey to investigate the significance of the perceived CAIS security threats is also different from that used in previous studies. In these studies, no criteria or clear guidelines, which might guide their perception (such as the frequency of occurrence of the threat, or the expected loss resulting from an occurrence of the threat), were given to respondents. Accordingly, the classification might vary from one respondent to another according to their knowledge, available data, personal perception of the threats, personal characteristics (optimistic, nonoptimistic), and the criteria used to formulate their judgment and make decisions. Given that prior studies obtain responses from multiple industries, this problem is likely exacerbated.

The current research, in contrast, investigates the significance of CAIS security threats through surveying their perceived frequency of occurrence during the previous year. The frequency of occurrence was used as a proxy for the materiality, importance of each CAIS security threat. It could be argued that a single occurrence of a security threat might cost the bank only a few dollars in one case but could cost several millions of dollars in other cases. Nevertheless, the occurrence frequency of a security threat is a critical measure for the following reasons:

- It is very difficult to obtain an accurate estimation of financial security losses related to the occurrence of each security threat because most banks are reluctant to report their financial losses; and
- According to Williams (1995), any type of security breach, however minor, can become disruptive and expensive, so it makes better business sense to take a preventive approach. The sooner action is taken to safeguard information systems, the better it will be for an organization in the long run.

IV. THE RESEARCH METHODOLOGY

A survey using a one-page self-administered questionnaire (Appendix) was conducted to investigate the opinions of the heads of internal audit departments (HoIAD) and the heads of computer departments (HoCD) in the EBI regarding the significant security threats challenging their CAIS. The respondents were asked to indicate the frequency of occurrence of each security threat by selecting one among five available choices: less than once a year; once a year to once a month; more than once a month to once a week; more than once a week to once a day; and more than once a day. The questionnaire was written and administered in Arabic. The translation of the questionnaire was tested by independent back-translation from the Arabic to English and back again to Arabic, showing close correspondence of the terminology and meaning of questions. Reliability tests using Cronbach's Alpha, show that the questionnaire is highly reliable regarding the frequency of occurrence of security threats (alpha = 0.7885).

The entire population (66 bank headquarters) of the EBI was surveyed in this research. Seventy-nine completed and usable questionnaires were collected from 46 different banks' headquarters. Forty-six of these questionnaires were completed by the heads of the computer departments, and 33 questionnaires were completed by the heads of internal audit departments. The response rate by bank type is illustrated in Table 1.

The response rate of the computer departments (after excluding merged, liquidated, too distant, and noncomputerized banks) was 79.3 percent, while the response rate was 56.9 percent from the internal audit departments. Both are considered high response rates. Each

TABLE 1
The Response Rate of the Headquarters Sample

The Bank Type	Total Number of Egyptian Banks		Responding Banks				Respondents type	
	Initial Number	Revised Number	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[a]	2	50	2	66.7	2	2
Commercial Private Banks	23	22[b]	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[c]	9	45	9	64.3	9	8
Total	66	58	46	69.7	46	79.3	46 (79.3%)	33 (56.9%)

[a] Two specialized public banks were merged into one bank.
[b] One bank was too distant to visit.
[c] Three banks were under liquidation, two banks had noncomputerized systems, and in one bank the researcher was not able to meet the target respondents.

banking category is represented in the sample. It is observed that 93.3 percent of the joint venture banks and 86.5 percent of the commercial private banks participated in this survey. Moreover, 64.3 percent of the local headquarters of foreign banks, 50 percent of commercial public banks and two-thirds of specialized public banks are involved in the research sample and data analysis.

Furthermore, the researcher carried out an unstructured interview to explore the respondents' opinions regarding the relative importance of CAIS security threats, the financial security losses that occurred in the last 12 months due to internal and external actions, and the adequacy of implemented security controls used to prevent, detect, and correct such security breaches in their banks

The data were analyzed using the Statistical Package for Social Sciences (SPSS), version 12. Descriptive statistics (such as frequencies and percentages) of the collected data were calculated to gain an understanding of the main research variables. Nonparametric tests (such as the Kruskal-Wallis test and Mann-Whitney test) were used to investigate significant differences among different bank types as well as differences between respondent groups (HoCDs and HoIADs) regarding their perceived security threats to CAIS in the EBI. Nonparametric tests, rather than parametric tests, are the most appropriate statistical tests for analyzing data collected in this research since these tests do not require the data to be normally distributed and can efficiently deal with small samples. Nonparametric tests are also suitable to analyze nominal, ordinal, categorical, and scale ranked data (see: Dickinson 1990; Miller 1991; Hessler 1992; Melville and Goddard 1996; Wackerly et al. 1996; Abu-Musa 2003b).

V. RESULTS

Accidental Entry of Bad Data by Employees

Overall, respondents saw the accidental entry of bad data to be relatively frequent. Of those responding, 70.8 percent indicated that accidental entry of bad data by employees occurs more than once a month. Only four respondents (5.1 percent) indicated a frequency of occurrence less than once a year. 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 2).

Intentional Entry of Bad Data by Employees

The findings show that the majority of respondents (73.4 percent) believe that the intentional entry of bad data by employees happens very rarely in their banks, being likely to occur even less than once a year. They consider it to be a crime (i.e., computer fraud) and believe that whoever commits such a crime should be prosecuted. Only one respondent believes that intentional entry of bad data by employees happens relatively frequently in his bank. He believes it might occur more than once a month to once a week, due to the large, scattered number of the bank's branches and the inadequacy of implemented controls.

Accidental Destruction of Data by Employees

Slightly more than half of the respondents (54.4 percent) believe that the frequency of accidental destruction of banks' data as a result of employees' errors or mistakes is less than once a year. Thirty five percent of the respondents indicate that accidental destruction of banks' data could happen between once a year and once a month and only 10 percent of respondents believe that it might happen more than once a month to once a week. When the respondents were interviewed, one mentioned that it would not be surprising if such

TABLE 2
The Frequencies of CAIS Security Threats

Accounting Information Systems Threats	Less than once a year		Once a year to once a month		More than once a month to once a week		More than once a week to once a day		More than once a day (or more 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	45	57.0	24	30.4	5	6.3	3	3.8	2	2.5
8. Introduction entry of computer viruses to the system	57	72.2	18	22.8	4	5.1	0	0	0	0
9. Natural disaster such as fire, flooding, loss of power	56	70.9	21	26.6	2	2.5	0	0	0	0
10. Human-made disasters such as fire, floods, explosions, and loss of power	59	74.7	19	24.1	1	1.3	0	0	0	0
11. Suppression or destruction of output	62	78.5	15	19.0	1	1.3	1	1.3	0	0
12. Creation of fictitious/incorrect output	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	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 them	51	64.6	26	32.9	1	1.3	1	1.3	0	0
18. Sensitive documents are handed to nonsecurity-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

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 is an inconsequential threat, however, because data can be easily recovered through the bank's back up system.

Intentional Destruction of Data by Employees

The results show that the great majority of the respondents (92.4 percent) believe that intentional destruction of data by employees very rarely occurs in their banks occurring less than once a year. When it happens, it is often triggered by embezzlement. Thus, it is observed that the frequency of intentional data destruction is quite low in the EBI.

Unauthorized Access to Data and/or System by Employees

The majority of the respondents (85 percent) claimed that unauthorized access to their banks accounting systems rarely happened, occurring less than once a year, due to secure password systems. Unauthorized access to the banks' accounting systems/data by employees seems to be an infrequent security threat in the EBI.

Unauthorized Access to Data and/or System 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. One possible interpretation of this result is that electronic banking services (such as phone banking, electronic fund transfer, and corporate-banking) are not widespread and accepted in the EBI. However, 24 percent of the respondents believe it happens more than once a year. Two respondents (representing 2.5 percent of responses) believed that unauthorized access to the data system by outsiders (hackers) happened more than once a month to once a week, one respondent indicated that it occurred more than once a week to once a day, and one respondent affirmed that it happened more than once a day in his bank (Table 2).

Introduction (Entry) of Computer Viruses to the System

The reported frequency of computer viruses is quite low in the EBI. The majority of respondents (72.2 percent) reported that the introduction of computer viruses occurs less than once a year whereas approximately 23 percent of the respondents believed that it happens more than once a year to once a month. The possible reason behind the infrequent occurrence of viruses could be that the majority of Egyptian banks use mainframe computer systems, booting the original programs and software packages, and almost all use diskless computers.

Natural Disasters

The results showed that the majority of respondents (approximately 71 percent) confirm the rarity of natural disasters (including loss of power) in the EBI. Such natural disasters as earthquakes or loss of electricity occasionally happen, but less than once every several years. Moreover, floods and wind disasters very rarely occur in Egypt. Almost 29 percent of the respondents believed that they happen once a year to once a week.

Disasters of Human Origin

Man-made disasters include fires, floods, and explosions. The results reveal that approximately one-quarter of the respondents believe that man-made disasters occur more than once a year.

Employees' Sharing of Passwords

Slightly more than half of the respondents (57 percent) believe that sharing of passwords occurs less than once a year whereas 43 percent of respondents reported that sharing occurs more than once a year.

Suppression or Destruction of Output

The majority of respondents (78.5 percent) believe that suppression or destruction of their banks' output occurs less than once a year. Only two respondents, representing 2.6 percent of the total, believe that suppression or destruction of their banks' output occurs more than once a month (Table 2).

Creation of Fictitious/Incorrect Output

The majority of respondents (88.6 percent) believe that creation of fictitious/incorrect output rarely happens, occurring less than once a year. Fictitious or incorrect output does not appear to be a security concern in the EBI.

Theft of Data/Information

The majority of the respondents (approximately 80 percent) indicate that theft of data/information is rare in their banks, since it occurs less than once a year. However, 20 percent of the respondents believed that it happens once a year to once a month.

Unauthorized Copying of Output

Most respondents (91.1 percent) believe that unauthorized copying of output is rare, believing that it occurs less than once a year.

Unauthorized Document Visibility

The majority of respondents (83.5 percent) believe that unauthorized document visibility, by displaying it on monitors or printed on paper, is very rare, as it occurs less than once a year, while a substantial minority (15.2 percent) believe that it occurs once a year to once a month. One respondent believes that it happens more than once a month to once a week in his bank. According to the above result, unauthorized document visibility seems to be a very low level threat in the EBI.

Unauthorized Printing and Distribution of Data/Information

Most respondents (87.3 percent) consider the frequency of unauthorized printing and distribution of information to be extremely low in their banks (less than once a year). However, 12.7 percent of respondents believe that it happens between once a year to once a month.

Directing Printouts and Information to People Not Entitled to Receive Them

Two-thirds of respondents (64.6 percent) indicated that misdirection of printouts and distributed information to individuals not entitled to receive them is very rarely encountered in their banks (less than once a year). However, 33 percent of the respondents believe that it happens once a year to once a month. Two respondents (2.6 percent) mentioned that it occurs either once a year to once a month or more than once a week to once a day.

Sensitive Documents Handed to Nonsecurity-Cleared Personnel for Shredding

The vast majority of respondents (92.4 percent) reported that handing sensitive documents to nonsecurity-cleared personnel for shredding very rarely occurs in their banks.

Interception of Data Transmissions

The majority of respondents (82.3 percent) consider that interception of data transmissions very rarely occurs in their banks; however, 16.5 percent of respondents reported that it occurs once a year to once a month and one respondent believes that data transmissions are intercepted more than once a month to once a week.

Between-Respondent Comparisons

The results tend to provide evidence of consistent perception regarding the significance CAIS security threats across EBI. The results of the Kruskal-Wallis test (Table 3) show no significant differences between different bank types regarding the occurrence frequency of CAIS security threats in the EBI, except for the unauthorized access to data and/or CAIS by outsiders (hackers) natural disasters, man-made disasters, and theft of data and information (at significance level $p = 0.05$). It is also observed that off-shore banks and banks which offer Internet and phone banking services reported higher perceptions of such security threats compared to other banks.

Although Egypt is not an active area for volcanoes, earthquakes and other natural disasters, the research findings surprisingly show that natural (nonhuman) disasters are perceived as one of the significant security challenges in the EBI. Moreover, the results of

TABLE 3
The Results of Kruskal Wallis Test of CAIS Security Threats

Accounting Information Systems Security Threats	Chi-Square	df	Asymp. Sig
1. Accidental entry of bad data by employees	1.709	4	.789
2. Intentional entry of bad data by employees	5.662	4	.226
3. Accidental destruction of data by employees	1.949	4	.745
4. Intentional destruction of data by employees	.896	4	.925
5. Unauthorized access to the data and/or system by employees	2.835	4	.586
6. Unauthorized access to the data and/or system by outsiders (hackers)	11.632	4	.020
7. Employees' sharing of passwords	3.995	4	.407
8. Introduction (entry) of computer viruses to the system	3.768	4	.438
9. Natural disaster such as fire, flooding, loss of power	11.834	4	.019
10. Human-made disasters such as fire, floods, explosions, and loss of power	15.154	4	.004
11. Suppression or destruction of output	3.089	4	.543
12. Creation of fictitious/incorrect output	8.361	4	.079
13. Theft of data/information	9.306	4	.054
14. Unauthorized copying of output	1.984	4	.739
15. Unauthorized document visibility by displaying on monitors or printed on paper	1.644	4	.801
16. Printing and distribution of information by unauthorized persons	1.111	4	.892
17. Prints and distributed information are directed to people who are not entitled to receive them	6.436	4	.169
18. Sensitive documents are handed to nonsecurity-cleared personnel for shredding	3.145	4	.534
19. Interception of data transmissions from remote locations	1.986	4	.738

the Kruskal-Wallis test (Table 3) show no significant differences between different bank types regarding the frequency of occurrence of such security threats in the EBI (at significance level $p = 0.05$). 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.'' Interviewing the respondents clarified such confusion, the respondents believe that nonhuman security threats of CAIS includes not only natural disasters (such as floods, earthquakes, or failure of a power supply of the CAIS) but also nonhuman security threats related to technical threats to the IT (such as technical failure of the system or hard disk failures) and other IT technical facilities (such as software problems).

On the other hand, the results of the Mann-Whitney test (Table 4) show significant differences between the opinions of the HoIAD and the HoCD regarding the frequency of occurrence 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 EBI. In all these cases, the HoIAD reported a higher rate of frequency of occurrence 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 2002; Hunton et al. 2004), 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.

Interviewing the respondents revealed that many of the surveyed banks suffered from financial security losses due to disgruntled or dishonest employees and external (hackers) actions. The financial security losses ranged from 50,000 to 250 million Egyptian pounds and many banks were reluctant to report their actual losses. The respondents also mentioned that, even in cases where computer-related frauds were discovered and the perpetrator identified, banks were reluctant to involve the police. Banks believe that reporting these incidents would negatively affect their reputation and indicate weakness in their CAIS to shareholders, potential customers, and competitors.

VI. 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 EBI. A proposed list of CAIS security threats was developed based on the previous studies (e.g., Loch et al. 1992; Davis 1996; Ryan and Bordoloi 1997) and other available literature in this area. However, some security threats were suggested and included in this list to be investigated for the first time. The results show that accidental entry of bad data by employees, accidental destruction of data by employees, introduction of computer viruses to the system, natural and human-made disasters, employees' sharing of passwords and misdirecting prints and distributing information to unauthorized people are the most perceived significant security threats to CAIS in the EBI. The results provide further evidence that the greatest security concerns are perceived to come from within, not without the bank (Loch et al. 1992; Davis 1996; Weingartner and Burton 1991; Jenkins et al. 1992; Schultz 2002; Carnevale 2003; Green 2003; Swann 2004).

The results are consistent with the opinion of the Organization for Economic Cooperation and Development (OECD) (1996) stating that employees who have been granted authorized access to the information systems pose a larger threat. 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

TABLE 4
The Results of Mann-Whitney Test of CAIS Security Threats

Accounting Information Systems Security Threats	Mann-Whitney U	Wilcoxon W	Z	Asymp. Sig. (2-tailed)
1. Accidental entry of bad data by employees	606.000	1687.000	−1.608	.108
2. Intentional entry of bad data by employees	724.500	1285.500	−.447	.655
3. Accidental destruction of data by employees	500.000	1581.000	−2.891	.004
4. Intentional destruction of data by employees	699.500	1260.500	−1.289	.197
5. Unauthorized access to the data and/or system by employees	758.500	1319.500	−.008	.994
6. Unauthorized access to the data and/or system by outsiders (hackers)	605.500	1686.500	−2.048	.041
7. Employees' sharing of passwords	589.500	1670.500	−1.899	.058
8. Introduction (entry) of computer viruses to the system	751.500	1832.500	−.095	.924
9. Natural disaster such as fire, flooding, loss of power	742.000	1823.000	−.214	.831
10. Human-made disasters such as fire, floods, explosions, and loss of power	650.000	1731.000	−1.436	.151
11. Suppression or destruction of output	731.500	1812.500	−.383	.702
12. Creation of fictitious/incorrect output	673.500	1754.500	−1.543	.123
13. Theft of data/information	628.000	1709.000	−1.871	.061
14. Unauthorized copying of output	716.500	1797.500	−.858	.391
15. Unauthorized document visibility by displaying on monitors or printed on paper	655.000	1736.000	−1.608	.108
16. Printing and distribution of information by unauthorized persons	647.500	1728.500	−1.924	.054
17. Prints and distributed information are directed to people who are not entitled to receive them.	668.500	1749.500	−1.079	.281
18. Sensitive documents are handed to nonsecurity-cleared personnel for shredding	741.000	1822.000	−.390	.697
19. Interception of data transmissions from remote locations	717.000	1798.000	−.630	.528

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) confirms that ''creating a secure environment is complicated by the fact that workers must support security efforts for them to be effective, but it is often employees that pose the greatest threat to security. Most workers, however, are not actively trying to breach security. Often, careless mistakes and indiscriminate access to information are at the root of security problems. Therefore, the more informed users are, the more likely they are to accept the policies.'' Again, Wood and Banks (1993) state that human error is one of

the major and most serious threats to information security that is often ignored or dismissed as inevitable. This type of thinking runs counter to reality, since studies have shown that with the right professional assistance, human errors could be easily corrected or significantly reduced. According to Haugen and Selin (1999) unintentional acts, while costly at times, could be corrected, or avoided through training and supervision.

Intentional acts such as the 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 also include manipulative activities such as deleting or altering records and files to remove damaging information or create false information. According to the results of the current study, intentional acts such as these happen less frequently relative to other threats.

The results of Kruskal-Wallis tests (Table 3) show that there are no significant differences between different bank types regarding the frequency of occurrence of CAIS security threats in the EBI, except for the unauthorized access to data and/or CAIS by outsiders (hackers, natural disasters, man-made disasters, and theft of data and information). However, the results of the Mann-Whitney test (Table 4) show nonsignificant differences between the opinions of the HoIAD and the HoCD regarding the frequency of occurrence of security threats, except for accidental entry of bad data by employees, accidental destruction of data by employees, employees sharing passwords, and unauthorized printing and distribution of data and information in the EBI. In all these cases, the HoIAD reported a higher rate of frequency of occurrence of CAIS security threats than the HoCD.

In interpreting the findings, it is important to consider the potential limitations of this research. First, frequency of occurrence was used as a proxy for the importance of each CAIS security threat. Future research is needed to relate security threats to monetary exposure. Second, the current research was implemented in the banking sector and may not extend to other industries or other countries. Third, the current research is focused on the banks' headquarters in the EBI. Further research could be extended to the bank branch level. It would be interesting to explore whether the banks face the same security threats throughout the organizational hierarchy. 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.

APPENDIX
The Questionnaire

1. ***Do you currently work in: (Please, tick)***

- ☐ **Public Sector Bank**
  - ☐ Commercial Bank
  - ☐ Specialized Bank
- ☐ **Private Sector Bank**
  - ☐ Commercial Bank
  - ☐ Business and Investment Bank
    - ☐ *Private or Joint bank*
    - ☐ *Offshore bank*

2. ***Please indicate the frequencies of each threat by ticking the appropriate place:***

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

REFERENCES

Abu-Musa, A. A. 2003a. The perceived threats to the security of computerized accounting information systems. *The Journal of American Academy of Business* 3 (1): 9–20.

———. 2003b. *Evaluating the Security Policies of Computerized Accounting Information Systems*: *Evidence from the Egyptian Banking Industry*. The 28th International Conference of Statistics, Computer Science, and Its Applications, Cairo, Egypt (April 12–17).

Carnevale, W. 2003. Awareness of computer-security threats is still inadequate. *Chronicle of Higher Education* 50 (12): 30–32.

Coffin, R. G. and C. Patilis. 2001. The internal auditor's role in privacy. *Internal Auditing* 16 (2): 22–28.

Davis, C. E. 1996. Perceived security threats to today's accounting information systems: A survey of CISAs. *IS Audit Control Journal* 3: 38–41.

———. 1997. An assessment of accounting information security. *The CPA Journal* 67 (3): 28–34.

Dhillon, G. 1999. Managing and controlling computer misuse. *Information Management & Computer Security* 7 (4): 171–175.

Dickinson, J. P. 1990. *Statistical Analysis in Accounting and Finance*. London, U.K.: Philip Allan.

Federal Financial Institutions Examination Council (FFIEC). 1996. *IS Examination Handbook, Chapter 14, Security-Physical and Data Workprogram.* Washington, D.C.: Government Printing Press.

Green, M. 2003. Securing the system. *Best's Review* 103 (10): 80–84.

Haugen, S., and J. R. Selin. 1999. Identifying and controlling computer crime and employee fraud. *Industrial Management and Data Systems* 99 (8).

Hessler, R. M. 1992. *Social Research Methods*. New York, NY: West Publishing Company.

Hermanson, D. R., M. C. Hill, and D. M. Ivancevich. 2000. Information technology-related activities of internal auditors. *Journal of Information Systems* 14 (1) (Supplement): 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* 6 (3): 5–15.

Hunton, J., A. Wright, and S. Wright. 2004. Are financial auditors overconfident in their ability to assess risks associated with enterprise resource planning systems? *Journal of Information Systems* 18 (2): 7–28.

Jenkins, B., P. Cooke, and P. Quest. 1992. *An Audit Approach to Computers.* London, U.K.: Institute of Chartered Accountants in England and Wales.

Loch, K. D., H. C. Houston, and M. E. Warkentin. 1992. Threats to information systems: Today's reality, yesterday's understanding. *MIS Quarterly* (June): 173–186.

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

Miller, D. C. 1991. *Handbook of Research Design and Social Measurement.* 5th edition. London, U.K.: SAGE Publications.

National Institute of Standards and Technology. 1995. *An Introduction to Computer Security: The NIST Handbook*. Technology Administration, U.S. Department of Commerce Special Publication 800-12. Washington, D.C.: Government Printing Office.

———. 2003. *Standards for Security Categorization of Federal Information and Information Systems.* Computer Security Division, Information Technology Laboratory, Initial Publication Draft, Version 1.0. Washington, D.C.: Government Printing Office.

Organization for Economic Co-operation and Development (OECD). 1996. *Guidelines for the Security of Information Systems*. OECD Publishing.

Parker, D. B. 1976. *Crime by Computer.* New York, NY: Charles Scribner's sons.

Qureshi, A. A., and J. G. Siegel. 1997. The accountant and computer security. *The National Public Accountant* 43 (3): 12–15.

Ryan, S. D., and B. Bordoloi. 1997. Evaluating security threats in mainframe and client/server environments. *Information & Management* 32 (3): 137–142.

Schultz, E. E. 2002. A framework for understanding and predicting insider attacks. *Computers & Security* 21 (6): 256–531.

Smith, L. B. 1995. On the new beat. *PC Week* 12 (43): E1–2.

Swann, J. 2004. Always on the case: Engaging your staff in bank security. *Community Banker* 13 (3): 44–47.

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

Wackerly, D. D., W. Mendenhall, and R. L. Scheaffer. 1996. *Mathematical Statistics with Applications.* London, U.K.: Duxbury Press, Wadsworth Publishing Company.

Warren, M. J. 2002. Security practice: Survey evidence from three countries. *Logistics Information Management* 15 (5/6): 347–351.

Weingartner, A., and M. Burton. 1991. PC security—Don't be caught out. *Computer Security Guide:* 33–35.

White, G. W., and S. J Pearson. 2001. Controlling corporate email, PC use, and computer security. *Information Management & Computer Security* 9 (2/3): 88–93.

Williams, P. 1995. Safe, secure, and up to standard. *Accountancy*: 60.

Wood, C. C., and W. W. Banks. 1993. Human error: An overlooked but significant information security problem. *Computers & Security* 12 (1): 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* 16 (Supplement): 99–113.