Accounting and Management Information Systems
Vol. 17, No. 3, pp. 440-461, 2018
DOI: http://dx.doi.org/10.24818/jamis.2018.03006

The threats of using computerized accounting information systems in the banking industry

Ernest Amoaful Bansah[a,1]

[a]*University of Cape Coast, Ghana*

Abstract: The adoption and over dependence on IT in performing banking operations during the past decades are well-recognised. The use of information systems in performing accounting tasks has been credited with many accolades nonetheless, threats to the systems have become inevitable for most firms in the changing business environment. In this study, the extents to which CAIS in the banking industry in Ghana are susceptible to vulnerability are explored by means of descriptive survey. The study investigated the sources and causes of risks that threaten CAIS in financial firms and the preventive measures available to mitigate their occurrence. The study reveals that the most worrying sources of threats to CAIS include power outages, risks posed by employees, viruses, and threats from outsiders. With regards to the causes of risks to CAIS, the findings indicate that accidental entry of bad data, unauthorized copying of the system's output, lack of frequent back-ups, infrequently updates on system security software, access to data by unauthorized personnel, weakness in internal controls, and lack of written policies are the major causes of threats to CAIS. Generally, the findings indicate high level of perceived sources and causes of risks among financial firms in Ghana. However, effective measures to secure CAIS are lacking. It is therefore recommended that attention is given to these issues before they become unbearable.

Keywords: computerized accounting information systems, financial firms, threats, security controls

JEL codes: M41, M15

[1] *Corresponding authors*: College of Distance Education, University of Cape Coast, Ghana
email addresses: ernestamoafulbansah@gmail.com

1. Introduction

Financial firms are established for purposes such as mobilizing savings as well as providing credit services and facilities to customers. The customer (s) may be an individual, group of individuals or organizations. As the population increases and people develop savings and investment habit, the use of the traditional system of handling transactions by financial institutions makes it difficult to serve the needs of the numerous customers effectively and efficiently. Again, the provision and presentation of reliable information to serve the need and interest of the various user groups becomes difficult to achieve because of the huge data base that are made available from operations. As a result of these, many companies have taken advantage of the development in information technology (IT) and availability of user friendly accounting software applications to computerize their accounting information system. Similarly, increased competitions in the financial sector have compelled many institutions within the sector to computerize their systems in order to remain competitive.

The growing use and over dependence on information and communication technologies (ICT) in the financial sector during the past decades are well-noticed and unquestionable reality. Different groups of financial service providers have obtained very unique results in relation to the expected increase in productivity and in business performance due to large investments in information technology. This new trend has made it easier to handle the more difficult tasks that were cumbersome to perform through the traditional system (manual system). Its wider use in the performance of the various tasks in accounting has given opportunity to companies to move toward a paperless era. That is to say that, with the adoption of IT in business operations, the manual system of handling data is gradually being substituted. IT has now become the reason behind the growth of most organizations around the globe. It has been considered as the tool for knowledge since the search for relevant and reliable information for an effective decision is facilitated by its wider use in all fields of life.

The introduction of technology in accounting started in the early 20th century with the introduction of the first operational business computer (Fadzil *et al.*, 2005). Since then, a number of accounting software packages have been developed by software manufacturers to make accounting tasks less complex and more accurate. These software packages have made it easier for accounting tasks to be run on a computer system hence the name Computerized Accounting Information System (CAIS). Information provided by CAIS has been described with attributes such as reliable, adequate, and relevant. Nevertheless, threats to CAIS have become inevitable for most organizations in the changing business environment. According to the National Institute of Standards and Technology (2003), organizations that are using IT in their operations are more vulnerable to threats which could in effect

result in damages that may lead to significant financial loss. Stonebumer *et al.* (2002) categorized sources of these threats into natural threats, human based threats and environmental threats. The use of a computerized accounting information system in organizations in general and financial institutions in particular has been characterized with some of these challenges and security issues that threaten the safety of the system and the efficiency of its use.

The rapid advancement in information technology, the wide spread of user-friendly software applications and the over reliance on information system by organizations to perform their operations have increased security threats to the information system which in turn have affected business activities (Kankanhalli *et al.*, 2003; Abu-Musa, 2006; Salehi, 2010). Precisely, the growing reliant on the CAIS by financial institutions in executing its business activities have made it difficult to separate information technology (IT) from the business activities of these institutions.

It is clear that there are greater possibilities of threats to CAIS. These types of threats are common not only to the developed countries but also to the developing countries as well. As a result, adopting appropriate security control measures over the CAIS of an organization and its related peripherals has become an issue of concern to many organizations (Abu-Musa, 2004). Ghanaian companies cannot be left out of these security challenges. It is therefore anticipated that these challenges to computerized accounting information systems are prevalent in Ghanaian companies as well, therefore, the need for this study to critically evaluate the extent to which such risks manifest and the measures firms within the industry are currently putting in place to minimize their occurrence and effects. This present study is therefore centred on such challenges, hereafter referred to as 'risks', their perceived prevalence and threats to CAIS in the Ghanaian banking industry.

Although empirical studies on threats of CAIS have been studied in some part of the world (Abu-Musa, 2005, 2006; Hanini 2012), such studies have been limited to the causes of risks and security controls available to mitigate these risks. Analysis of existing literature shows that no study has explored the sources of risks that threaten CAIS. This paper seeks to bridge that gap and to bring knowledge of CAIS to the rest of the world, whilst providing findings that will provide immense assistance to Information system (IS) developers, security consultants, IT users and practitioners, and Managers of financial institutions to develop better understanding of the sources of threats to their systems and how best they will be able to secure their CAIS in a suitable manner to achieve their objectives successfully.

The position of the Ghanaian economy in the world of business, and the need to develop its accounting information systems, make Ghana a perfect location for this study. The Ghanaian experience is importance to the rest of the world and non-

Ghanaian readers for a number of reasons. First, computerization of non-commercial banks started in 2010 and currently, almost all financial institutions operating in Ghana are mechanized, making them more susceptible to cyber security theft. The spread of cybercrimes in Africa and Ghana in particular is on the ascendency. The news that Ghana is ranked among countries prone to cyber threats gives reason for a holistic approach aimed at combating unauthorized intrusions into financial information hereafter increasing the confidence of investors and other customers that their information will be secured, irrespective of how it is accessed.

To place Ghana's story in the context, it is necessary to examine the state of CAIS in the financial service industry especially non-commercial banks in the years leading up to the discovery of oil and expansions in businesses over the years. With the growing concerns that fraud within the financial service sector is on the rise, there is the need to assess the threats if any to the computerized systems and the pragmatic policy measures instituted to mitigate cyber incidences and crimes. Ironically, with all the security apparatus, the nation has fallen victim to cyber fraud in the past. Important national webpages like the National Communication Authority (NCA), the National Information Technology Agency (NITA), and the webpage of the vice president of Ghana have all been hacked in recent times (Ministry of Communications, 2014). A study by 3T Solutions Consulting titled "2017 West Africa Cyber Security Indexing and Readiness Assessment" gives evidence that even though some financial institutions in Ghana have security strategies targeted at mitigating cyber threat, others are still at risk. The information offered through this study will provide the prospect of using CAIS to improving performance.

Second, it is also important to create awareness of security threats and develop methodologies and strategies that will help lessen the risks associated with CAIS. In line with the assumptions outlined earlier on, this study seeks to examine the sources and the perceived causes of risks that subject CAIS to vulnerability and the preventive measure currently in place to protect CAIS by financial firms.

2. Financial service sector in Ghana

Financial service delivery has undergone a lot of changes over the past decades. The manual accounting system dominated past banking activities therefore creating long queues and inconvenience in banking halls. Modern banking in Ghana started in the late 19th century with dominance from Standard Chartered and Barclays bank. The British Bank of West Africa, now the Standard Chartered Bank, was established in Ghana about 122 years ago, followed by Barclays Bank which has been in operation since 1917. These two banks were subsidiaries to their parent banks incorporated in the United Kingdom.

In 1935, farmers' co-operatives and the colonial government established the co-operative bank to finance farming activities especially cocoa buying and facilitating the activities of co-operative societies in the country. Prior to independence, the Bank of the Gold Coast was also established. The Gold Coast Bank which was partly owned by the government managed government activities while providing banking services to farmers and acting as an agent in the floatation of government bonds. After independence in 1957, the Bank of Gold Coast was split into Bank of Ghana and Ghana Commercial Bank. The Bank of Ghana assumed central banking activities whilst the commercial banking activities were supervised by the Ghana Commercial Bank.

The post-independence era saw a lot of banks emerging and providing financial services in Ghana. Currently, the country can boast of about 33 licensed banks of which 16 are locally owned and 17 foreign controlled (PWC, 2017). Included in these banks is ARB Apex Bank, which is the central bank for rural and community banks operating in the various rural communities in Ghana. There are about 140 licensed and registered rural and community banks at the various regions in Ghana.

3. Computerization of banking activities in Ghana

The earliest Information and Communication Technology devices adopted in the financial service sector in Ghana were telephones, telex and facsimile (Abor, 2004). These devices were used together with the manual system to facilitate banking operations and to ensure accuracy and efficiency in delivering financial services. As banking operations became intensified and competitive, the use of the traditional means of serving customers lost its relevance. With advancement in technology, computers paved way for banks to network their activities thereby enabling computerization of banking and accounting systems.

The most innovatory computerized electronic facility used in Ghana and most part of the world to perform basic banking functions such as issuing cash withdrawals and cash deposits is the Automatic Teller Machine (ATM). Banks with ATM facilities also have their banking operations networked hence making them more useful to their customers. The first universal bank to install ATM in 1995 was the Trust Bank, now a member of the Ecobank group, followed by the Ghana Commercial Bank and Agricultural Development Bank in 2001. Today all banks registered and licensed by the Central bank have their banking operations computerized. This has enabled cheque clearing system which is mainly a computer-based over a Wide Area Network (WAN).

To enhance rural banking through Information Technology, the Ghana Rural Banks Computerization and Interconnectivity Project (GRBCIP) financed by the United

State government through the Millennium Challenge Account (MCA) was instituted to ensure mechanization of rural and community banks operating under the ambit of the ARB Apex Bank limited. The project commenced in 2010 with over 500 VSAT WAN sites installed all over Ghana with a state-of-the-art data unit. The project saw rural banks migrating unto the Temenos eMerge T24 platform.

In the next section of the paper, general literature on computerized accounting information system is reviewed. This is followed by a description of the method adopted for the study and the discussion of the study's results. In the concluding section of the paper, recommendations are made.

4. Literature review

4.1 The nature of accounting information system

The accounting system of most organizations is largely linked to the various administrative processes. The system helps in making decisions, performing the administrative functions and raising the levels of performance in order to achieve corporate goals (El-Dalabeeh & Alshebeil, 2012).

Accounting Information System (AIS) has been described by many researchers. In 1966, the American Institute of Certified Public Accountants (AICPA) opined that: "Accounting actually is information system and if we be more precise, accounting is the practice of general theories of information in the field of effective economic activities and consists of a major part of the information which is presented in the quantitative form". Boockholdt (1999) defined accounting information system as systems that collect, process and categorize data and report financial events with the aim of providing relevant information for decision making purposes.

As an important aspect of management information system, accounting information system processes financial data or transactions and provides financial information and reports to managers for planning and controlling current and future activities whilst assisting stakeholders with reliable information for rational decision making.

4.2 History of accounting information system

Before 1970 and 1980, the most commonly used accounting information system was the general ledger, thus the manual system. Daily transactions were recorded by hand into a journal and then posted to the general ledger account before financial statements could be prepared. These processes were noted to be slow and inaccurate since mistakes in the process took too long in detecting and correcting (Hous, 2013).

Through the 20th century, revolution in the Information and Communication Technology (ICT) brought a positive influence on the accounting processes. The first use of the term "computerized accounting information system" became known in the 1920's but Scholars during that period conceded that, the development of CAIS's had even begun earlier. For instance in 1890's, calculating machines, like Hollerith device were invented to meet the needs of cost accountants (Badua & Watkins, 2013).

The introduction of user friendly business software packages changed the processes involved in the accounting cycle. Accounting operations that was performed manually were replaced with computers in most organizations. A countess Ada Lovelace computing device was the first to be developed and used for accounting duties. The IBM 9Pac was one of the earliest business software packages that were developed before the invention of many modern accounting software packages (Novinson, 2013). In 1973, SAP software program was released and updated in 1975 to include features that enabled businesses to do purchasing, inventory management and other accounting related tasks automatically.

During the period of growth and development of information technologies in accounting, the manual system of handling accounting data was substituted for computerized system and these made the work of accountants and businesses less difficult and more productive. Business owners, who had limited knowledge in accounting, could manage their accounting duties with available software packages (Hous, 2013).

4.3 Threats to CAIS

Horan (2017) pinned, no organization is safe from computer security threats. Technological advancement has created an avenue for cyber criminals to exploit the CAIS of organizations. The researcher identified hackers, viruses, spyware, adware, phishing, worms, spam, rootkits and Denial-of-Service (DOS) attack as among the various types of computer security threats. According to the Australian Computer Society (2016), computer security threats exist in various forms spanning from Denial-Of-Service attack on websites, extortion, data manipulation, blackmail, theft and destruction. The tools usually used include malware, ransomware, social engineering and spyware. Malware is still a common threat to CAIS but the past decade is marked with the emergence of threats like fileless attacks, encrypted infiltrations and credential thefts which are more challenging to identify (McAfee Labs 2015). The findings of Verizon (2017) recognized 10 threat actions that pose risk to CAIS. The study identified misdelivery, publishing errors, disposal errors, misconfiguration, omission, programming error, malfunction, Gaffe, data entry error as manmade threat to CAIS.

According to Tanya *et al.* (2018), theft of corporate information, unauthorised access by outsiders, employees' misuse of internet access privileges and viruses are common threats to CAIS. Wahab (2003) also attest that computer virus is one of the threats and restrictions of the computerized system.

A lot of studies have used various empirical approaches to investigate threats to CAIS in most part of the world, for instance, in China (Hood & Yang, 1998); Jordan (Zweilf, 2009; Hanini, 2012); Egypt (Abu-Musa, 2005); Nigeria (Muhrtala & Ogudeji, 2013); Kenya (Polo & Dima, 2013). The findings of Hong and Yang (1998) revealed human security threats particularly malicious attack from outsiders as the most significant security threats facing Chinese banking industry. In British, Australian and American firms, Waren (2002) established weakness of technological security procedures as a significant challenge of information systems in British and Australian firms but wrong entry of financial data into the system as the problem among American firms.

The findings of Zweilf (2009) corroborates Abu-Musa (2005) that unintentional and intentional entry of bad data, unintentional destruction of data by employees, employees' sharing of passwords, introduction of viruses to the computer system, unauthorized visibility of documents are amongst security threats to CAIS. Other studies suggest that accidental entry of bad data by employees, accidental destruction of data by employees, employees sharing of log-on credentials, introduction of virus into the system, unauthorized access to information and unauthorized documents visibility through display on the screen are the major security threats to computerized accounting information systems (Muhrtala & Ogundeji, 2013).

Criminal activities undertaken through computers and the internet continue to threaten organizations and it is financial institutions that usually fall victims to these increasing threats. Findings from PWC's Global Economic Crime Survey (2016) shows that 54% of organizations in the world have been threatened via fraudulent and other economic crime activities. This crime rate dropped to 49% in 2018 when a similar study was carried out by PWC. It is obvious that some organizations are more vulnerable to these cyber-attacks than others. Studies show that one of the target organizations for cybercrimes is the banks. PWC (2014) ranked cybercrime as the second most common type of economic crime that threatens banks. About 65% of the total fraud cases reported by financial institutions are technology related (PWC, 2015). Cyber-attacks are marshalled through payment cards, debit and credit cards, and technological devices like the ATM's. In India for instance, banks offering online banking services usually become susceptible to computer threats (PWC, 2015). In Zimbabwe, hacking, phishing, identity theft and malware are the major types of cybercrimes in financial institutions (Mugari *et al.*, 2016).

These crimes are targeted at financial institutions and are invariably done for financial gains. In UK, cyber criminals broke into Tesco Bank's CAIS and stole over £2.5 million from the account of about 9000 customers (Raymond & Liisa Lahti, 2017). In 2016, Distributed Denial- of- Service (DDoS) attack threatened the Britain's HSBC, one of the largest banks in the world and brought it operations to a stalemate. This rendered online banking services inaccessible to customers. The Bangladesh Central Bank also suffered cyber threat when the central bank's security system was hacked and the perpetrators transferred $101 million unto another account in other countries (Karim, 2016). Debatably, Asian banks appear as the most vulnerable to these cyber threats. Financial institutions in countries like the Philippines, Japan, Taiwan, Thailand and Vietnam recently became victims to cyber threat (Jones, 2016). In 2016, over 100 organizations in 31 countries in the financial sector had their CAIS threatened (Symantec, 2017).

4.4 CAIS and firm's performance

Several studies in different countries have addressed the role of a computerized accounting information system on the performance of the various activities within the organizational set up. In United Arab Emirate (UAE) for instance, computerized accounting information systems have helped companies to develop a better relationship with their clients. Development in computerized system has helped companies to save time in processing transactions (www.ameinfo.com). The adoption of CAIS have brought about development in the financial, administrative performances and an improvement in decision making processes in the financial sector as they provide methods and tools which help in evaluating performance and making productive decisions (Santhanam & Hartono, 2003; Naesa & Khamees, 2009).

In countries like Finland, Iran, Malaysia, Spain, Pakistan and Jordan, prior studies have also shown that computerized accounting information system have helped increase firm's performance, profitability, efficiency in operations and reduce cost (Gullkvist, 2002; Sajady *et al.*, 2008; Kharuddin *et al.*, 2010; Grande *et al.*, 2010; Kouser *et al.*, 2011; El-Dalabeeh & Alshebeil, 2012).

4.5 Security controls

Security controls refers to tools that provide security services, for example passwords and firewalls. Information systems security control is a means of ensuring business continuity and minimizing business damage by preventing and mitigating the effect of threats to the system (Dhillon, 1995; von Solms, 1998). Existing literature have identified a number of security control measures necessary to mitigate threats to the CAIS. These control measures have been categorized into physical controls; technical controls and administrative controls.

Dougan (1994) suggested the following security controls: minimizing physical dangers in the computer room; maintaining the computer systems and safeguarding the system files. Dougan therefore categorized these security control procedures into Computer room site (physical access); Documentation; Maintenance; and Protection. Qureshi and Siegel (1997) proposed physical access controls (identification, passwords and cards/keys), and communication security controls like Line security, Transmission security, Digital signature, Cryptographic security, Emission security and Technical security as effective security controls. The researchers further classified security controls into Deterrent; Preventive; Detective; and Corrective controls.

The findings of Hood and Yang, (1998) revealed that information security was inadequate in the Chinese banking sector. Nonetheless, password, daily backup and observing network activities were found as the major security controls in the Chinese banking sector. In Moscove, (2001) the researcher discussed E-business security and controls and suggested some control procedures to protect computer systems from threats and unauthorized access to include: Physical access; Password; Data encryption; Disaster recovery; Software-based security; and Intrusion detection software to monitor computer system and its parts.

In 2008, the office of the Secretary of Defense in the United State (US) mandated the National Security Agency (NSA) to prioritize a list of security control measures to assist the Department of Defense (DoD) rank its cyber security spending. A consortium led by John Gilligan of Centre for Internet Security (CIS) and Alan Paller of SANS institute also participated in a public-private partnership to provide the same control-prioritization knowledge as provided to the DoD for civilian government agencies. The membership of the consortium was expanded to include the United Kingdom's Communications Electronics Security Group (CESG) and Centre for the Protection of National Infrastructure (CPNI), the DoD Chief Computer Network Architect, Defense Cyber Crime Center, three Department of Energy (DOE) laboratories, and companies like McAfee and Lockheed. The consortium unanimously agreed on 20 critical controls that can address the most prevalent threats found in government agencies and industries.

These security controls have since been accepted, adopted and implemented by many organizations and departments in the world. For instance in 2009, the United State Department of State certified the consensus security control measures. In December 2011, the United Kingdom's Centre for the Protection of National Infrastructure (CPNI) notified the UK government agencies and industries about the government adoption of the 20 critical security controls. The Commander of the US Cyber Command and Director of NSA said, the adoption of the security controls was a good basis for effective Cyber Security. The Idaho National

Laboratory, in June 2012 completed a positive analysis of how the 20 critical security controls applied in the electric sector (SANS Cyber Defence, 2014).

Although considerable efforts are being made by security agencies to help mitigate the losses from cyber security threats, the security control measures put in place are outpaced by advancement in technology (Mugari *et al.*, 2016). Cybercriminals are continually exploring new ways of attacking computer users.

5. Research methodology

Descriptive survey design was adopted in this study. The population of the study consisted of financial firms operating in Ghana. The scope of the study was however limited to firms within the Kumasi Metropolis and its environs. These firms included rural banks, savings and loans, and micro-finance institutions. Though the firms were the unit of analysis, data from each firm was gathered from two groups: the head of IT department and the branch manager. A quota sampling technique was adopted in selecting the banks.

In all, 30 firms were considered for the study. At least five firms from each category of financial institution responded to the survey instrument, with at most two responses each coming from the head of IT and the branch manager.

Data from the target respondents were gathered with the aid of self-administered questionnaires. Based on the study's objectives and materials reviewed for the study, the questionnaire items were mainly close-ended. The nature of the questionnaire items were typically structured using five (5) point likert scale, some of which range from 'strongly disagree' to 'strongly agree' and 'not at all' to 'to a greatest extent'. The questionnaire items were presented in four (4) headings: Respondents and firms background information, Sources of risks that threaten CAIS, Causes of risks that threaten CAIS, and Preventive measures.

Quantitative method was employed in analyzing the data gathered. In this regard descriptive analysis techniques were used. Frequencies, percentages, means, and standard deviations became relevant in the analysis. The analyses were also performed with the support of Statistical Package for Social Scientists (SPSS) and Microsoft Excel.

5.1 Quality of the study

Quality concerns in empirical investigation tend to be addressed by the concepts of validity and reliability (Bergman & Coxon, 2005). "Reliability and validity are tools of an essentially positivist epistemology."(Watling, as cited in Winter, 2000; Golafshani, 2003). Patton (2002) also asserts that validity and reliability are two

elements which any qualitative researcher should be particular with while planning a study, analysing results and judging the quality of the study. Joppe (2000) defines reliability as the extent to which the study results are consistent over time and produce an accurate representation of the total population under study. Validity determines the extent to which the research measures that which it was intended to measure (Joppe, 2000).

To improve on the reliability of the data for the study, most of the questionnaire items were in the structured form, making more use of Likert scales. To enhance the validity of the data gathered, the initial data gathering instruments developed were thoroughly examined by IT practitioners. A pilot test was also conducted to ensure that the respondents adequately understand the questionnaire items. Inputs gathered from the pilot study helped in refining the questionnaires to ensure that they gather data for which the study's research questions required.

5.2 Ethical considerations

Prior to the study, ethical clearance was obtained from the Managements of the selected financial institutions. Approval relating to the data collection from the respondents was also sought. As a result, two areas of ethical concerns were appreciated during the research. Thus, informed consent and privacy assurance prior to the actual data collection. These concerns were addressed by first writing officially to the Executive Directors of each selected financial institution requesting management consent to undertake the research in the institution and its affiliate branches.

Before the questionnaires were administered to the participants, the respondents were assured that the names of the institutions would remain confidential. Hence the respondents of the various institutions were requested to willingly participate in the study. In this regard, the anonymity of the respondents was assured.

5.3 Limitations and delimitations of the study

The main limitation of the study is the sampling technique adopting in selecting the financial institutions. These institutions were sampled based on a quota. A probability sampling technique would have ensured equal chances given to the target respondents. However, for survey studies, since there is a perceived less variability in responses, and for practicality reasons, the quota technique adopted became appropriate. The study is delimited to the participation of three categories of financial firms in Ghana. Financial firms within the universal banking category were not included.

It became difficult making contacts and seeking approvals from the headquarters of most of the financial institutions earmarked for the study. Executive directors of some targeted institutions were reluctant to grant authority to their staff and branch officers to participate in the study. Some management were categorical as it is against their corporate ethics to engage in surveys. Branch officers who have sworn oath of secrecy were also hesitant in contributing to the study.

Due to the busy schedules for banking activities, it became difficult obtaining responses from all the two respondent groups, as a result, the response rate on the part of the managers particularly was smaller.

6. Results and discussion

The overall responses expected to be received was 60, however, 49 were duly gathered from the various institutions. This represented 81.67% response rate. The breakdown of the firms' and the respondents' demographics is given in table 1.

Table 1. Demographic and firm breakdown

		Count	Percent
Gender	Male	41	83.7%
	Female	8	16.3%
Status	Head of IT	28	57.1%
	Branch Manager	21	42.9%
No. of years spent with this firm	5 or less	39	81.2%
	Above 5	9	18.8%
Bank category	Rural bank	12	24.5%
	Micro-finance	21	42.9%
	Savings & Loans	16	32.7%

6. Findings

This subsection provides general statistics and discussions on the variables considered relevant to attaining the objectives of the study.

6.1 Sources of risks that threaten CAIS

In this study, six (6) main forms and sources of risks that threaten CAIS were identified to include risks posed by employees, viruses, power outages, natural disasters, intentional disasters, and threat from outsiders. On a scale of 1 to 5, where 1=not at all and 5=to a greatest extent, the respondents were asked to rate the degree to which their systems are believed to be susceptible to these sources of risks. Table 2 shows the results from these evaluations.

Table 2. Sources and forms of risks that threaten CAIS

	Mean	Mode	Standard deviation
Power outages	3.67	4	0.996
Viruses	3.53	4	1.231
Employees	3.22	3[a**]	0.985
Natural disasters	3.13	3	1.142
Threat from outsiders	3.13	3	1.160
Man-made disasters	3.04	3	1.098

** a. Multiple modes exist. The smallest value is shown

The mean scores of responses given in table 2 indicate that CAIS in financial firms within the study's scope are more prone to system damages resulting from power outages, followed by viruses, and employees. However, given a mean score greater than 3.00 indicates that, generally, the respondents perceive that all these factors, to some extent could be sources of risks that threaten CAIS in the industry.

6.2 Causes of risks that threaten CAIS

For ease of assessment, the specific causes of risk were broadly categorized into three (3) areas: Activities and Actions of Employees, Weakness in System Security and Preventive Measures, and Weakness in Controls and Standards. The results from these assessments are given in tables 3a, 3b, and 3c.

6.2.1 Employee activities and actions

Results given in table 3a generally indicate numerous possible causes of risks that threaten CAIS resulting from employees' activities and actions in the financial firms understudied. This is because, all risk variables identified to cause threats to CAIS have mean values more than 3.00, indicating that the respondents agree to the fact that these are possible causes of threats to their systems.

Table 3a. Employee activities and actions

	N	Min.	Max.	Mean	Std. Dev.
Bad data entered unintentionally by employee	47	2	5	3.87	0.900
Making unauthorized copies of system files	49	2	5	3.78	0.896
Bad data entered intentionally by employee	48	1	5	3.73	1.125
Unintentional entry of virus	49	1	5	3.69	1.194
Lack of commitment	49	2	5	3.65	0.991
Incompetent employees recruited	48	2	5	3.54	1.202
Unintentional damage of files by employees	49	1	5	3.45	1.138
Intentional damage of files by employees	49	1	5	3.43	1.190
Intentional entry of virus	49	1	5	3.33	1.125

Variable weights: 1=strongly disagree, 2=disagree, 3=indifferent, 4=agree, 5=strongly agree

The most cause of vulnerability to CAIS with regards to the activities and actions of employees was found to be bad data entered unintentionally by employees (M=3.87, N=47, SD=.900). This could probably mean that either the people employed in the industry are perceived to be incompetent or lack skills and knowledge on how to man the systems or enter right data onto the system. This is followed by the chances that employees will make unauthorized copies of the system's output (M=3.78, N=49, SD=.896). Notwithstanding this, the respondents also perceive the likelihood of workers intentionally entering bad data (M=3.73, N=48, SD=1.125) onto the system. The reason for this is better associated with the issue of commitment (M=3.65, N=49, SD=.991) which the respondents consider as a potential threats to CAIS in their firms.

6.2.2 Weakness in system security and preventive measures

Risks springing up from weakness in system security and preventive measures were also perceived and found to be several. Causes of these risks include: the prevalence of infrequent file backups (M=3.71, N=48, SD=1.1166), not frequently updating the system's security (M=3.69, N=49, SD=1.122), access by unauthorized personnel (M=3.64, N=49, SD=1.182), the use of inappropriate firewalls and antivirus (M=3.63, N=48, SD=1.044), etc. Per the scale of the respondents' scores, all these were perceived to be causes of risks that threaten CAIS in the industry, given that their means scores were more than 3.00.

Table 3b. Weakness in system security and preventive measures

	N	Min.	Max.	Mean	Std. Dev.
Lack of frequent back-ups	48	1	5	3.71	1.166
Not frequently updating system security	49	1	5	3.69	1.122
Access to data by unauthorized personnel	49	1	5	3.65	1.182
Inappropriate firewall/antivirus	48	1	5	3.63	1.044
Internet exposure (virus)	49	1	5	3.53	1.243
Common share of password	49	1	5	3.51	1.210
Lack of training	48	1	5	3.35	1.194

Variable weights: 1=strongly disagree, 2=disagree, 3=indifferent, 4=agree, 5=strongly agree

6.2.3 Weakness in controls and standards

In relation to controls and standards put in place to minimize risks that threaten CAIS, the responses indicate that, weakness in their internal control structures (M=3.75, N=48, SD=1.082) could be the main possible cause of risks that subjects CAIS to vulnerability. This is believed to be followed by lack of written policies on systems' security issues (M=3.65, N=49, SD=1.182). The least possible cause of

risks to CAIS in the industry is observed to be lack of standard protocols for sharing and sending files (M=3.39, N=46, SD=1.064).

Table 3c. Weakness in controls and standards

	N	Min.	Max.	Mean	Std. Dev.
Weakness in internal controls	48	2	5	3.75	1.082
Lack of written policies	49	1	5	3.65	1.182
Weakness in internal auditing activities	49	1	5	3.59	1.059
Lack of standard protocols	46	1	5	3.39	1.064

Variable weights: 1=strongly disagree, 2=disagree, 3=indifferent, 4=agree, 5=strongly agree

6.3 Preventive measures followed in safeguarding CAIS

The possible preventive measures that could safeguard CAIS were classified to include: policies, controls and resourcing, and security measures. On a scale of 1 to 5, the respondents were asked to make assessments on the extent to which their firms are currently making efforts on these dimensions in minimizing risks that threaten CAIS. The results given in table 4 indicate that, generally, financial institutions within the study's scope do poorly on measures needed to safeguard CAIS. All the mean scores were below 3.00, indicating some level of disagreement to the availability of these preventive measures required to mitigate the level of risks that threaten CAIS.

In all, the average respondent perceived that the use of common password, inappropriate firewall and antivirus, antivirus not updated frequently, employees lacking competence, lack of training for employees on how to effectively man the system, weak internal controls, ineffective internal auditing practices, infrequent backups of system files, lack of security policies and lack of protocols for sharing and sending files are the challenges to the security of CAIS in the industry under consideration.

Table 4. Preventive measures followed in safeguarding CAIS

	N	Min.	Max.	Mean	Std. Dev.
Security Measures					
Common share of password is not allowed	49	1	5	2.43	1.118
There is appropriate firewalls and antivirus	48	1	5	2.35	0.956
Antivirus is updated frequently	49	1	5	2.37	1.131
Control and Resourcing Measures					
Employees recruited are competent	49	1	4	2.65	1.147
Employees are adequately trained	49	1	5	2.61	1.239
There is strong internal control	47	1	5	2.28	1.097
Internal auditing activities are effective	48	1	4	2.42	1.007
There is frequent backups for system files	49	1	5	2.24	1.199

	N	Min.	Max.	Mean	Std. Dev.
Policy Measures					
Appropriate policies regarding system security	49	1	5	2.43	1.099
Existence of protocols for sharing and sending files	48	1	5	2.69	1.133

Variable weights: 1=strongly disagree, 2=disagree, 3=indifferent, 4=agree, 5=strongly agree

7. Conclusions

There is no argument about the immense contributions and benefits brought into the financial industry following the emergence of CAIS. Today, with the growth and adoption of CAIS there has been enhancement in administrative works, decision making, client satisfactions and increases in overall operations. Notwithstanding these, it is also clear that there are greater possibilities of risks that pose threats to CAIS. Evaluating the nature of such risks and the preventive measures adopted by firms in the financial firms was therefore timely, which occasioned the need for this study.

Findings of the study indicated the existence of perceived high level of risks emerging from employees, frequent power outages in the country, viruses, threats from outsiders, natural disasters, and disasters driven by human activities. Also, with regards to the respondents' perceptions on the specific causes of these risks, it was revealed that the industry's systems are prone to numerous risks factors, some of which includes bad data entered unintentionally by employees, employees making unauthorized additional copies of the system's output, lack of frequent back-ups, infrequently updates on system security software, access to data by unauthorized personnel, weakness in internal controls, and lack of written policies. The finding is in agreement with those of Zweilf (2009), Abu-Musa (2005) and Muhrtala & Ogundeji (2013). In terms of the industry's current efforts made towards securing CAIS, it was found that, less efforts are being made with respect to restricting the use of common share of passwords, putting in place appropriate and updating firewalls and antivirus, recruiting competent employees, training employees frequently, ensuring effective internal controls and audits, backing up system files, adopting appropriate policies and protocols for sharing and sending files.

However, on the basis of the findings and conclusions reached, it is recommended that certain measures need to be implemented to eliminate weaknesses and strengthen security controls against the threats of using CAIS. According to Horan (2017), the utmost defence mechanism against computer threat is education and training. Management should provide continuous security awareness training and education programs for new and existing employees to equip them with the importance of their commitment to control measures concerning the safety and security of the firms systems. This help keep employees awake on security threats

to the system and to thwart attacks. The requirement to acquire an uninterruptible power supply (UPS) by financial firms to protect their CAIS from frequent power outages is recommended. This emergency power supply has the capacity to provide power for a limited time to allow for effective shutting of computers during a power outage.

In order to keep the CAIS safe there is the need to do more than simply installing an antivirus program once and leaving it alone. It is very essential to update the antivirus software frequently to sure that it has all the information it needs to fight the most recent threats. There is the need to put proper protocols in place to ensure that valuable information which could be stolen, corrupted, deleted by a virus is secured. It must be noted that cyber criminals are always looking for means to create new and more powerful viruses. As a result, if the antivirus software is not updated against the most recent viruses that have been created, then the organization may be exposing itself to attacks.

Hacking is one of the most known forms of computer crime. In this context, it refers to the unauthorized access to another person's information. Hackers hack into company's information systems for financial benefits and to access personal information and files of others. It is recommended that company's remain alert and adopt a comprehensive security measure including file sharing and data management solutions to safeguard information system. The Ghanaian legislative must institute clear legislatures and deterrent penalties regarding cybercrimes to scare people from unauthorised access and intrusion of information systems for which they do not have authority over. Again, sensitive data stored should be encrypted by management of the financial institutions to reduce the chances of unauthorized access or exposure to people who do not have the right to access files.

Advancement in regulations in the financial service sector is necessary to help curb the threats to CAIS among players in the financial service community. With cyber threats now demonstrating to be a major challenge for financial institutions around the world, there is the need for the industry players to seriously raise their defence mechanisms to compensate for the losses and to control the emergence of subsequent threats. Stronger collaboration among banks globally and security agencies can significantly help to effectively counter threats to CAIS. Terrorizations these days are global, refined, and effectually organized. To effectively fight it, the financial community and law enforcement agencies must create open relationships, and develop new ways to effectively share information when threat ensues.

References

Abor, J (2004) "Technological innovations and banking in Ghana: An evaluation of customers' perceptions", *American Academy of Financial Management*, vol. 1: 1-16

Abu-Musa A.A. (2005) "Investigating the perceived threats of CAIS in developing countries: An empirical study on Saudi organizations", *Computer and Information science*, vol. 18: 1-26

Abu-Musa, A.A. (2006) "Exploring perceived threats of CAIS in developing countries: the case of Saudi Arabia", *Managerial Auditing Journal*, vol. 21 (4), 387-407

Abu-Musa, A.A. (2004) "Investigating the security controls of CAIS in an emerging economy: An empirical study on Egyptian banking industry", *Managerial Auditing Journal*, vol. 19(2), 272-302

ACS (2016) "Cybersecurity: threats, challenges, opportunities". Available from https://www.acs.org.au/content/dam/acs/acs publications/ACS_Cybersecurity_Guide.pdf [Accessed 0n 21st March 2018]

Badua, F.A. & Watkins, A.L. (2013) "Too young to have a history? using data analysis techniques to reveal trends and shifts in the brief history of accounting information systems", *Accounting Historians Journal*, vol. 38(2), 75-103

Bergman, M. M. & Coxon, A.P.M. (2005) "The quality in qualitative methods" *Forum qualitative sozialforschung / forum: Qualitative Social Research*, vol. 6(2)

Boockholdt, J (1999) *Accounting Information Systems Transaction Processing and Control*, London: Mac-Graw-Hill companies

Dhillon, G. (1995) *Interpreting the Management of Information Systems Security*, London: London School of Economics and Political Science.

Dougan, J. (1994) "Internal control check-list for hospitality computer systems", *The Bottom Line*, vol. 9 (5): 8-11

El-Dalabeeh & Alshebeil, (2012) "The role of computerized accounting information systems in reducing the costs of medical services at King Abdullah University Hospital", *Interdisciplinary Journal of Contemporary Research in Business*, vol. 4(6): 893-900

Fadzil, F.H.,Haron, H & Jantan, M (2005) "Internal auditing practices and internal control System", *Managerial Auditing Journal*, vol. 20 (8): 844-866

Golafshani, N. (2003) "Understanding reliability and validity in qualitative research", *The Qualitative Report*, vol. 8(4), 597-606

Grande, U.E., Estebanez, P.R. & Colomina, M.C. (2010) "The impact of Accounting Information Systems (AIS) on performance measures: Empirical evidence in Spanish SMEs", *The International Journal of Digital Accounting Research*, vol. 11: 25-43

Gullkvist, B. (2002) "Towards paperless accounting and auditing", E-Business Research Center, Finland

Hanini, E. (2012) "The risks of using computerized accounting information systems in the Jordanian banks; their reasons and ways of prevention", *European Journal of Business and Management*, vol. 4(20): 53-63

Hood, K.L. & Yang, J.W. (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 (3): 5-15

Horan M. (2017) "Main types of computer security threats that harm your company", Available from https://blog.ftptoday.com/main-types-of-computer-security-threats-that-harm-your-company [Accessed on 22nd March 2018]

Hous, C. (2013) "How have computerized accounting systems such as QuickBooks changed the way accounting is done?", ehow.com, Demand Media, Inc, Web., 18 March 2013

Joppe, M. (2000) "The research process", *The Quantitative Report Journal*, vol.8 (4): 597-607

Kankanhalli, A., Toe, H., Tan, B. & Wei, K. (2003) "An integrative study of information systems security effectiveness, international", *Journal of Information Management*, vol. 23 (2): 139-148

Kharuddin, S., Ashhari, M.Z. & Nassir, M.A. (2010) "Information system and firms' performance: The case of Malaysian Small Medium Enterprises", *International Business Research*, vol. 3(4): 28-35

Kouser, R., Awan, A., Rana, G. & Shahzad, F. (2011) "Firm size, leverage and profitability: Overriding impact of accounting information system", *Journal of Management and Business Review*, vol. 1 (10): 58-64

McAfee Labs (2015) "2016 threats predictions," available at www.mcafee.com

Ministry of Communications (2014) "Ghana national cyber security policy and strategy", Final Draft

Moscove, S.A. (2001) "E-Business security and controls", *CPA Journal*, 71 (11)

Mugari, I., Gona, S., Maunga, M., Chiyambiro, R. (2016) "Cybercrime - the emerging threat to the financial services sector in Zimbabwe," *Mediterranean Journal of Social Sciences*, vol. 7 (3): 135-143

Muhrtala, T.O. & Ogundeji M. (2013) "Computerized accounting information systems and perceived security threats in developing economies: The Nigerian case", *Universal Journal of Accounting and Finance*, vol. 1(1): 9-18

Naesa, M.S. & Khamees, B. (2009) "The impact of the Accountants' participation in developing the systems in the success of these systems and the impact of their application on the financial performance of the companies", *Jordanian Journal for Business*, vol. 5 (2): 182-203

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

Novinson, E. (2013) "The history of computerized accounting.ehow.com", Demand Media, Inc.Web.15thMarch2013

Patton, M. Q. (2002) *Qualitative Research and Evaluation Methods* (3rd ed.). Newbury Park, CA: Sage Publications

Polo, J. & Oima, D. (2013) "Effects of computerized accounting systems on audit risk management in public enterprises: A case of Kisumu county, Kenya, *International Journal of Education and Research*, vol. 1(5): 1-10

Pwc (2014) "Global economic crime survey 2014," available at www.pwc.org

Pwc (2015) "Current fraud trends in the financial sectors," available at https://www.pwc.in/publications/publications-2010-11.html

Pwc (2016) "Global economic crime survey 2016," available at *www.pwc.com/crimesurvey*

Pwc (2018) "Global economic crime survey 2018", available at www.pwc.com/crimesurvey

Qureshi, A.A. & Siegel, J. (1997) "The accountant and computer security", *The National Public Accountant*, vol. 43(3): 12-15

Raymond and Liisa Lahti (2017) "Cyber-attacks on banks: the consequences of a loss of access to bank records," The Journal of International Banking and Financial Law, vol 32(3)

Sajady, H., Dastgir, M. & Hashemnejad. (2008) "Evaluation of the effectiveness of accounting information systems", *International Journal of Information Science and Technology*, vol. 6(2)

Salehi, M., (2010) "Usefulness of accounting information system in emerging economy: Empirical evidence of Iran", *Economics and Finance*, vol. 2(2), 186-195

SANS Cyber Defence (2014) "Top 20 critical security controls (online)" Available at: http://www.sans.org/critical-security-controls [Accessed on 24th February, 2014]

Santhanam, R. & Hartono, E. (2003) "Issues in linking information technology capability to firm performance", *MIS Quarterly*, vol. 27: 125-153

Sharmeen Karim S.S. (2016) "Cyber-crime scenario in banking sector of Bangladesh: An overview," *The Cost And Management*, vol. 44(2): 12-19

Stonebumer, G., Goguen, A. & Feringa, A. (2002) "Risk management guide for information technology systems", *Nist Special Publication*, vol. 800(30): 800-830

Symantec (2017) "Internet security threat report 2017," Mountain View, CA: Symantec Corporation

Tanya, T, Tanuj T, Sanjay T & Shikha T. (2018) "Cybersecurity: threats, challenges and opportunities", *Austin Journal of Forensic Science and Criminology*, vol. 5(1): 1076: 1090

Verizon (2017) "Data breach investigations report" (10th Edition), Available from http://www.verizonenterprise.com/verizon-insights-lab/data-breach-digest/2017/

Von Solms, R. (1998) "Information security management: the code of practice for information security management", *Information Management and Computer Security*, vol. 6(5): 224-225

Wahab, A. (2003) *An Approach to Accounting*, 2nd Edition", United States of America: Irwin McGraw Hill Publishers

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

Winter, G. (2000) "A comparative discussion of the notion of validity in qualitative and quantitative research" *The Qualitative Report*, 4(3&4): 1-14

Zweilf, A. (2009) "The Nature of the threats of the electronic accounting information systems: An application study of the Jordanian insurance companies Arabian", *Journal of Accounting*, 46-64

WEBOGRAPHIES

http://www.ameinfo.com

http://ir.csuc.edu.gh:8080/xmlui/bitstream/handle/123456789/83/COMPUTERISD.pdf?sequence=1

http://theseus56kk.lib.helsinki.fi/bitstream/handle/10024/64144/thesis_bernard_adomako.pdf?sequence=1&isAllowed=y

http://dergipark.gov.tr/download/article-file/256783