Journal of Applied Economics and Business Research
JAEBR, 7(1): 01-17 (2017)

Role of Accountants and Auditors in Mitigating Digital Crimes

A. Seetharaman[1]
S P Jain School of Global Management, Singapore.

Nitin Patwa
S P Jain School of Global Management, Dubai.

Indu Niranjan
S P Jain School of Global Management, Singapore.

Abstract

In the new millennium, computers continued to play an ever-increasing role and presumed that the problems of computer frauds and crimes would also continue to persist and grow. So, long as the cyber criminal's ingenuity exists, any audit program may eliminate the probabilities of fraud only, but not possibilities of fraud. The Audit profession has responsibility for designing and developing an audit system to detect, deter and prevent computer frauds and crimes within an organization. This process will have an impact on the role, responsibility, authority, and liability of auditing profession. The introduction of effective auditing policies, procedures and tools can assist to mitigate organizational risks and maximize audit effectiveness. Auditors also must possess a sound knowledge of the subject matter audited and a requisite knowledge of information system and computer technology to conduct a continuous audit and to detect and prevent computer fraud. This article will explore the existence of computer crimes and frauds within an organization, and the methods adopted by audit profession to detect and prevent them in the future.

Key Words: Cybercrime, Computer Crime, Information security.

1. Introduction

Computer Crimes and frauds identified as unauthorized theft, use, access, modification, copying and destruction of software or data and theft of money by altering computer records or theft of computer time. There are various types of computer frauds and abuse techniques associated with white – collar crimes. In this context, the auditors play a vital role in detecting, preventing and reporting computer frauds. Auditors who specialize in fraud auditing and investigations are known as the forensic accountants. The forensic accountants are auditors trained in Information Technology Security Control Knowledge. These specialized auditors need to detect and prevent frauds to protect the information system of an organization. Auditors have to make use of fraud prevention techniques by making fraud less likely to occur, by increasing the level of difficulty for committing frauds by improving detection methods, by reducing fraud losses and finally identifying sufficient appropriate audit evidence to sentence fraud perpetrators with penalties upon the white-collar crimes. The need for computer forensic tools was stressed

[1] Correspondence to Nitin Patwa, Email: nitin.patwa@spjain.org

by Narayanan & Ashik, (2012) in the wake of increased cybercrimes annually. The authors advocated computer forensic analysis tools to be used in a legal setting. The growth of computer technology and the wide range of usage of computers will increase the risks of computer frauds and crimes, while auditors would play the role of “Computer Crime and Fraud busters” with the primal duty to detect and prevent computer crimes and frauds in the present and also in the future.

1.1 Research Problems

Computer Crimes and frauds identified as unauthorized theft, use, access, modification, copying and destruction of software or data and theft of money by altering computer records or theft of computer time. There are various types of computer frauds and abuse techniques associated with white – collar crimes. In this context, the auditors play a vital role in detecting, preventing and reporting computer frauds. Auditors who specialize in fraud auditing and investigations are known as the forensic accountants. The forensic accountants are auditors trained in Information Technology Security Control Knowledge. These specialized auditors need to detect and prevent frauds to protect the information system of an organization. Auditors have to make use of fraud prevention techniques by making fraud less likely to occur, by increasing the level of difficulty for committing frauds by improving detection methods, by reducing fraud losses and finally identifying sufficient appropriate audit evidence to sentence fraud perpetrators with penalties upon the white-collar crimes. The need for computer forensic tools was stressed by Narayanan & Ashik, (2012) in the wake of increased cyber crimes annually. The authors advocated computer forensic analysis tools to be used in a legal setting. The growth of computer technology and the wide range of usage of computers will increase the risks of computer frauds and crimes, while auditors would play the role of "Computer Crime and Fraud busters" with a primal duty to detect and prevent computer crimes and frauds in the present and also in the future.

1.2 Objective of Research

The objectives of the research are:

a) To explore the role, responsibility authority and accountability of auditors to detect, deter, discover and prevent computer crimes.
b) To equip auditing profession with necessary skills for designing, developing, choosing and monitoring effective computerized auditing systems (software) to detect, deter, signal, discover and prevent computer frauds and crimes.
c) To protect the computer system and data from unauthorized access or misuse of confidential information by theft, alteration, modification, falsification and destruction by providing and ensuring security provisions.
d) To ensure effective coordination between internal auditors and external auditors in controlling and dealing with computer frauds and crimes.

2. Literature Review

Computer crimes defined as “A criminal act that has been committed using a computer as a principal tool.”

Further, a distinction drawn between computer related fraud and computer assisted fraud. In a computer, related fraud the computer is purely coincidental whereas in computer assisted fraud

 ISSN 1927-033X

the computer is used to commit the fraud. Basically, in every computer crime, a computer has either been the object, subject or instrument of crime. (Taylor, Fritsch, and Liederbach, 2014) in their text have shown growing problems of crime, terrorism and information warfare being committed using computer technology.

Theft of money, information, tapping into data transmission lines, theft of goods by their diversion to the wrong destination or it may be theft of computer time i.e. use of an employer's computer resources for personal work. Malware (viruses, worms, and Trojans) still are the most dominant regarding reported incidents. These findings reconcile well with other studies; virus attacks are still the most prevailing incidents (FBI, 2005, PWC, 2006) and it has in fact been the number one threat for over eight years (Whiteman, 2004b) The above techniques apparently cover major forms of computer crime. Computer crime can take the form of authorized use or access to the information system or the modification of program to benefit the fraudster (Holt and Bossler, 2013). (Taylor, Fritsch, & Liederbach, 2014) in their text introduces about types of crimes, acts of terrorism, and information warfare that are committed using computers and networks.

According to the article, computer crime can also be in the form of hacking, sabotage and burgle involves breaking into other people's systems for fun or with the intent to blackmail or commit sabotage. Although the article attempts to explain forms or types of computer and computer related crimes (Fraud), an attempt to list computer crimes are exhaustive, and it is futile to provide a complete or definite list. Warwick (1997) argues on "whether hacking can be classified as white collar crime or not?" He lays down the difference between hacking and criminal hacking. In explaining whether computer crimes such as hacking and criminal hacking constitute "white collar crime," the author used a decided case of Kevin Mitnik. Straub (2009) classified theses are security policy violators as "white hat" and "black hat." A majority of computer crimes occur because a current employee of an organization has subverted existing controls (Dhillon, Moores, 2001)

"White collar violations are those violations of law to which penalties are attached that involve the use of violator's position of significant power, influence or trust in the legitimate economic or institutional political order for the purpose of illegal gain, or to commit an illegal act for personal or organizational gain." In labeling Kevin Mitnik, as white collar criminal, the author attempted to establish, whether Kevin's hacking activity done in the course of his occupation, whether Kevin were holding high social status at the time of the crime and hacking into to several computer systems done for economic gain. As all the answers are negative, Kevin neither tagged as white collar criminal nor hacking in any way classified as white collar crime. Further, the author made a distinction between "hacking" and "criminal hacking," although the legislators seriously undermined both "hacking" and "criminal hacking." For instance, here are three types of behavior that warrant the term criminal nature of the offense:

a) The behavior is so serious that goes beyond what dealt with by compensation, and regulation should be in the interest, i.e. the idea of crime against society.
b) The behavior is the sort where any sanction less than a criminal one would be ineffective, impracticable or insufficient. The use of criminal sanction helps to maintain public respect for the law.
c) The behavior should be possible to enforce the offense. Therefore, if the said offense of hacking falls with ambits mentioned above, then it is a criminal offense in contrast with civil wrong.

 ISSN 1927-033X

Denning (1990) in his article had conducted a detailed survey on hackers. His findings suggest that hackers are learners and explorers who want to help rather than cause damage, and who often have very high standards of behaviors. The author suggested that hackers have an intense, compelling interest in computers and learning, and many go into the computer as a profession. Some hackers break into systems to learn more about how the system works. Hackers see a security hole and take advantage of it because it is there, not to destroy information or steal. He says it is analogous to someone discovering methods of acquiring information in a library and becoming excited and perhaps engrossed. He pointed out that hackers do have ethics, no doubts malicious hacking was normally wrong. Most hackers are not intentionally malicious, and they are concerned about causing accidental damage. Some hackers feel that certain break-ins were unethical such as, breaking into hospital systems, read confidential information about individuals or steal classified information. The author also suggested that hackers express concern about their negative public image and identity. He says that hackers often portrayed as being irresponsible and immoral. In fact, hackers want to help system managers make their system more secure. The system manager should recognize and use hacker's knowledge about design flaws and the outside threat problem.

In 1989, the co-founder of the Apple Computer Corporation made a donation to the University of Colorado for a computer hacking scholarship in the belief that it increased knowledge and understanding of computer system. However, such move would be disastrous and to encourage hacking activities in many computer systems such as the control of nuclear power stations, defense system, and air flight control may lead to terrorism.

Thompson (1998) outlined in detail information obtained from a complete survey on computer security. The Office of Strategic Crime Assessments (OSCA) and the Victoria Police Computer Crime Investigation Squad conducted the cyber crime and security survey to establish some reliable baseline information regarding the extent of computer-related crimes in Australia. The author's findings reveal that nearly 90(ninety) percent of computer-related incidents attacks from sources internal to their organization, and over 60(sixty) percent more subjected to intrusions from External sources. Author's survey in the form of a questionnaire and for over 300 companies. At the end of the survey, the author is of the opinion that most of the computer related incidents framed by internal sources of each organization and intruders with legitimate access means employees of the own organization.

Selin (1999) highlighted on computer crime and computer related crime in the workplace, and he provided some statistics about the growth of fraud, factors which cause fraud in the workplace and how businesses can protect their assets. The article also highlighted on common computer based frauds techniques and controls over it. His findings highlighted that no organization is immune today from both external and internal threats to the safety and security of their data and information. Security is one of the essential requirements for cyber facilities Peykanpourm & Jalali (2016) therefore; authors suggested that managers of all types of the organization need to be knowledgeable about their internal control system so that managers will be in a position to carry out check and balances to ward against employees committing fraudulent acts. The authors identified few factors that enhance the probability of fraud in the workplace which includes, inadequate rewards, management controls, reinforcement and performance

 ISSN 1927-033X

feedback mechanism, he also mentioned about lax enforcement of disciplinary rules and may be fostering hostility.

Baker (1999) in his article examines the issue of fraud on the internet and discusses three areas with significant potential for misleading and fraudulent practices i.e. Security Fraud, Fraud in electronic commerce and Fraud arising from the rapid growth of internet companies. The author highlighted that security frauds had been committed using the Internet include, an online investment newsletter, bulletin boards, and e-mail Spam. According to the author, most transactions involving electronic commerce connected to credit cards or bank charges. Polivanjuk (2001) highlighted on prevention of computer crimes in the banking industry. The author listed out four ways in which information security can be breached i.e. unauthorized access of information, use of collateral electromagnetic radiations and inducing, use of the laying devices and implementation of computer viruses and other ways of disturbance. He discussed in detail the main methods and means of engineering information security with the restricted access to the automated systems and means of computer engineering. The article highlighted that the primary means of information security involves physical measures, hardware means, software means, hardware and software means, cryptographic and organizational methods. Willison & Warkentin (2012) investigated and suggested IS security controls specifically deterrence safeguards in three areas - techniques of neutralization, rationalization, expressive/instrumental criminal motivation and disgruntlement as a result of perceptions of organizational injustice—and propose questions for future research in these areas.

The author also rightfully pointed out the main reasons that lead to committing computer crimes are such as:

a) The absence of attending personals activity control, which helps a criminal use a computer freely as the instrument of crime.
b) A low level of the software which has no reference security and does not ensure the inspection of conformity and accuracy of the information.
c) The imperfection of a password security system from the unauthorized access to a workstation or its software which does not provide authentic identification of a user according to individual biometrics parameters.
d) In the absence of strict approach to the employee’s access to the secret information.

Ritchey (1996) pointed out in her article that computer crimes account for losses of more than one billion dollars annually in the USA. A survey by the Computer Security Institute (CSI) Federal Bureau of Investigation (FBI) Computer Crime Division found that nearly half of the five thousand (5,000) companies, Federal Institutions and Universities polled experienced computer security breaches within the last twelve months. The author explained that computer crimes might take several forms such as sabotage, revenge, vandalism, theft, eavesdropping and even “data diddling” – the unauthorized altering of data before or after it is input into a computer system.

The author also discussed in detail on prevention of computer crimes and laid down certain safety and security measures such as - Store backup information, encryption of software, firewalls as security shield, virus detection programs, authentication devices, patented technology and audit trial. Dhillon & Moores (2001) computer crimes happen more often because of violations of safeguards by the employee.

 ISSN 1927-033X

Chula G. King and W. Timothy O'Keefe (2004) discussed the issue of the online theft. According to the authors, it is fast growing in the United States, and the perpetrator obtains personal information by way of social security number or stolen a credit card. Identity theft also includes stealing target business particulars, stealing of bank account number, employee and client information. The author's identified that perpetrator obtain lots of information about individuals from CPA firms publication of the e-mail addresses of their principals or employees. Such information could be detrimental to CPA firm clients and employees. Therefore, the CPA firms should weigh the benefits of making this information available online with the potential costs that could result if a web spoofer assumed the online identity of one or more of these individuals. A good balance between various kinds of controls would be essential in instituting a cost-effective means to make any misconduct difficult. Which ensures accountability where every possible individually for all potentially sensitive negative actions (Dhillon, Moores, 2001)

Moreover, with ID and password, the web spoofer could access confidential client information from the legitimate website. Therefore, firms should assess whether the benefits of allowing client login to outweigh the potential threat. The authors only highlighted that CPA firms publicize the e-mail addresses but, there are many other organizations and corporate companies do public e-mail addresses of clients and employees, which are vulnerable to the online identity theft. Therefore, the authors could have discussed in detail about other online email address displays for a comparative study.

2.1 Role of Auditors and Accountants

U.S. Department of Labor published an article which provides on nature of work of an accountant and auditor. Accountants and auditors help to ensure that the firms run efficiently, its public records kept accurately and on time. They perform these vital functions by offering an increasingly wide array of business and accounting services to their clients. The article further explains types of services provided by accounts and auditing such as public, management, government accounting and internal auditing.

a) Public accountants – also called as cost management, industrial, corporation, governments, nonprofit organizations, and individuals.
b) Management accountants – also called as cost management industrial, corporate or private accountant record and analysis the financial information of the companies for which they work.
c) Government accountants and auditors work – in the public sector, maintaining and examining the records of government agencies and auditing private businesses and individuals whose activities are subject to government regulations or taxation.
d) Internal auditors verify the accuracy of their organization's internal records and check for mismanagement, waste or fraud.

This article in explaining job outlook stressed that, as a result of the recent accounting scandals, Federal legislation has increased penalties and make company executives personally responsible for falsely reporting financial information. These changes improve the security of company finances and accounting procedures for accountants and auditors to audit financial records more thoroughly. Financial crimes such as embezzlement, bribery, and securities fraud are on the increase. Moreover, computer technology has made these crimes easier to commit, and it is on the rise.

 ISSN 1927-033X

Makkawi & Schick (2003) the authors in their article had surveyed on how auditors alter their audit program decisions in response to an increased likelihood of fraud risk. Their investigation consists of a survey on 48 auditors from five large CPA firm, on the type of audit procedures, they would adopt in response to an increased likelihood of material misstatements caused by fraud.

The auditors placed in a scenario that reflected changes in economic and industry factors that increase audit risk and typically require a re-evaluation of the audit program. The auditors also were asked to make choices as to which tests of balances and details and analytical procedures to perform. The results of the study indicate the following four points:

a) All auditors increased the performance of certain procedures.
b) Some auditors chose not to reduce any procedures.
c) A consensus existed on which procedures to increase both for the analytical review procedures and tests of balances and details.
d) There was less agreement on which procedures for those auditors who chose to reduce some Procedures.
e) The case was for both the analytical review procedures and tests of balances and details.

The limitation of this article is that the authors omitted to discuss in detail appropriate audit procedure on striking a balance between effectiveness and efficiency in detecting material misstatements caused by fraud. Auditors are sensitive to fraud, but sometimes in reality auditing being a competitive business may outweigh the auditor's from preventing material financial misstatement of fraud.

2.2 The Impact of Computer Crimes in Auditing Profession

Farrell & Franco (1999) the authors have done an extensive survey of certain accounting firms including "Big Six" solely about accounting profession and auditors. The authors are of the opinion that fraud and white collar crimes have increased considerably over last ten years and professionals believe this trend is likely to continue. The cost to business and public cannot be estimated, as many crimes go unreported. However, the statistics we currently have show astronomical values associated with fraud, moreover the expansion of computers into business may make organizations more vulnerable to fraud and abuse. The authors embark on auditor's role, to prevent fraudulent behavior such as cutting costs, spending corporate and share holder's money on personal expenses and manipulating financial records for personal needs. In outlining the auditor's role, the authors insisted that it is the responsibility of the auditor, to maintain codification of auditing standards and procedures.

"The auditor has a responsibility to plan and perform the audit to obtain reasonable assurance about whether the financial statements are free of material misstatement, whether caused by error or fraud. Because of the nature of audit evidence and the characteristics of fraud, the auditor can obtain reasonable, but not absolute, assurance that material misstatements are detected. The auditors have no responsibility to plan and perform the audit to obtain reasonable assurance that misstatements, whether caused by error or fraud that are not material to the financial statements are detected." The auditors are given several important roles by the authors to search for fraud in every auditing exercise and to act as "police or detective "when conducting an audit, along with CPA's and other codification of auditing standards and procedures. The author also imposes a responsibility on the management of the business to take every necessary step to combat fraud and

 ISSN 1927-033X

white collar crime in business. The article finally concluded that it is a concentrated effort by the management of the business, the external auditors and all the employees of the company to combat fraud and white collar crime.

Glover & Aono (1995) the authors have proposed a new model for fraud detection that goes beyond internal accounting control. Initially, internal and external auditors focus on internal controls and management integrity as the principal components to determine the propensity of irregularity. The authors are of the opinion that the historical approach is too narrow and will only provide a limited degree of post audit detection, they have revised the traditional audit risk model to provide a more proactive integrated approach to prevent and detect fraud. The new model creates an interaction between corporate culture and industry traits. The interaction of corporate culture and industry traits yield the overall effect of the client's management of style of the industry, if an auditor understands the corporate culture, he will better understand where, when, how and why fraud will occur. This new model requires the auditor to consider additional variables when reviewing the same set of background information to establish a level of materiality.

2.3 Preventive Measures Adopted Against Computer Crimes by Audit Profession

Clikeman (2003) discussed accounting ethics and ways to prevent future accounting scandals. The accounting firm requested on accounting educators to integrate the values of quality, integrity, transparency and accountability into the curriculum. As an accounting educator despite teaching the technical material, need to introduce future accountants the ethical standards of the profession. Sometimes, being an accounting student a sense of responsibility for honest reporting may exist, but once he joins the firm, the culture and common values of his business have more influence on accountant's behavior than do the moral lessons he learned in college. Accounting educators can affect the attitudes and ethical beliefs with which young analysts begin their career, but the influence of collegiate education fades over time. Therefore, accounting firms must develop cultures that elevate integrity and responsibility to the public above profit and growth if accountants are ever to regain the public trust.

The quality, integrity, transparency, and accountability in any profession would not sustain, without any legal sanction. Code of Ethics from college cannot always maintain in real life without any legal sanction. The author ought to have discussed in detail, about malpractices of accounting firms and severe legal punishments provided by laws and regulations to deter such malpractices. Kligmen (2003) defined people's behavior today and a few decades ago. According to the author, the last few decades have seen a tremendous change in the culture of people and corporate structure. Greed, insatiability, advance, the need to "beat the Market" and top the other guy's salary fee, bonus and so on have led to a lessening of the ethical behavior of the people. Saini et al. (2015) Restrictions or prevention of such threats depended on upon a proper analysis of attacker's behavior and understanding of the impacts.

In the “olden days” people behaved differently. They were happy to “make a living” and for the most part thought of honesty as a virtue; despite there were dishonest people. Today ethics is considered to be an old-fashioned concept. It's for the nerds of the world, the cowards, and the fuddy-duddies. Today if you’ve got talent, imagination, ego and even some brains, you can play the angles. If you have the gift of gab, you can sell anything. So, what if it’s a little shady. Just cover it up. However, the author insisted that Ethics is part and parcel of the accounting profession. During student time, the ethics of the profession were pounded into student’s heads by every

 ISSN 1927-033X

instructor, with or without the use of textbooks. Since there is a tremendous decline in people's attitude in general, ethics is an important factor to gain public trust. Based on people's attitude and accountant's behavior many schools have made ethics course a mandatory part of their business and accounting curriculum. Perhaps this will help the future generation of CPA'S on track in a profession that has always known as honest and ethical.

SS Kien (2000) described the career paths and market value of IS auditors and status that with the continuous applications of advanced IT in business information systems, the future seems bright with promising career paths for IS auditors. Siew claims that the IS auditing profession is a unique crossbreed between IT and audit and has unique career development issues. The work by Siew also describes the market value of information systems auditors in Singapore but not in other countries. The limitation of the literature is that it does not present sufficient supporting factors that are affecting the market value of IS auditing profession. The literature also fails to explain about the contribution of an IS auditor in the information system environment.

Beirstaker, Burnaby & Thibodeau (2001) raised issues regarding paperless audit system. Currently, audit clients increasingly shift to paperless systems and audit software is developed that allows auditors to complete most procedures online. To inspect online system auditors will have their primary audit tool and gather evidence electronically. Current Technologies such as electronic data interchange (EDI) image processing and electronic file transfer (EFT) will disappear eventually. The use of online audit software will free the auditor from many mundane audit tasks and allow the audit to use this time for higher level tasks such as understanding the client's business and assessing various risks. However, the shift from computer generated audit programs to audit software will take some time, during this period the auditors will have more time to address the complex issues that their clients face in the global marketplace.

Rezaee (2004) Conducts a study on public trust in audit profession; he suggested necessary measures and steps regain the public trust in audit profession. Recent numerous financial restatements are high public companies coupled with bankruptcies of major companies caused by reported financial statement fraud have eroded public confidence in the financial report and related audit functions. Therefore, restoring the public confidence, require considerable efforts by legislators, standard setting bodies, the business community and the accounting profession.

The article suggested various ways that the accounting profession can rebuild public trust in the financial report and related audit functions. All the suggestions required the audit profession to adhere closely to the guidelines provided by governing bodies like the SEC, AICPA, and supreme court findings to regain the public trust which had eroded recently.

The Sarbanes – Oxley Act 2002, which closely related to SEC implementation rules, was enacted to:

a) Improve corporate governance the quality of financial reports, and the effectiveness of audit functions;
b) Provide new disclosure requirements for public companies;
c) Create an independent regulatory structure for the accounting profession; and
d) Establish stronger criminal penalties for securities fraud.

 ISSN 1927-033X

The public trust in auditor's judgment plays a major role in accepting audit functions as value added services, which lend credibility to published financial statement. This trust can be enhanced by CPA's to focus their core value of integrity, objectivity, independence and competence.

Gaumnitz & Lere (2004) discussed in detail the operation of section 406 of the Sarbanes – Oxley Act, which requires publicly traded companies to disclose their internal code of ethics for the senior financial officer.

Section 406 requirement is to be met, by all publicly trading companies to comply with the law's requirement. A code of ethics can guide individuals who have novel ethical situations and serve as general statements of company expectations for individuals who face situations with ethical dimensions. One of the main purposes of Code of Ethics is that it enables the senior financial officer to handle situations such as conflict of interest. Contemporary American Society does not have a consistent ethic for addressing conflicts of interest. Codes of ethics of professional organizations adopt one of two ways to handle conflicts of interest. Some systems require the strict avoidance of conflict of the interest; others treat conflicts of interest as acceptable as long as they disclosed to affected parties. The code of professional conduct for CPA'S contains elements of both. Some compromise the appearance of independence; others do not impair independence but require disclosure and possible recusal.

3. Data and Methods

The analysis and findings presented in this project drawn from secondary sources. The information gathered from business magazines, academic journal, and books. Internet used for getting updated information. The research framework for discussion, analysis, and findings are shown in Figure: 1

 ISSN 1927-033X

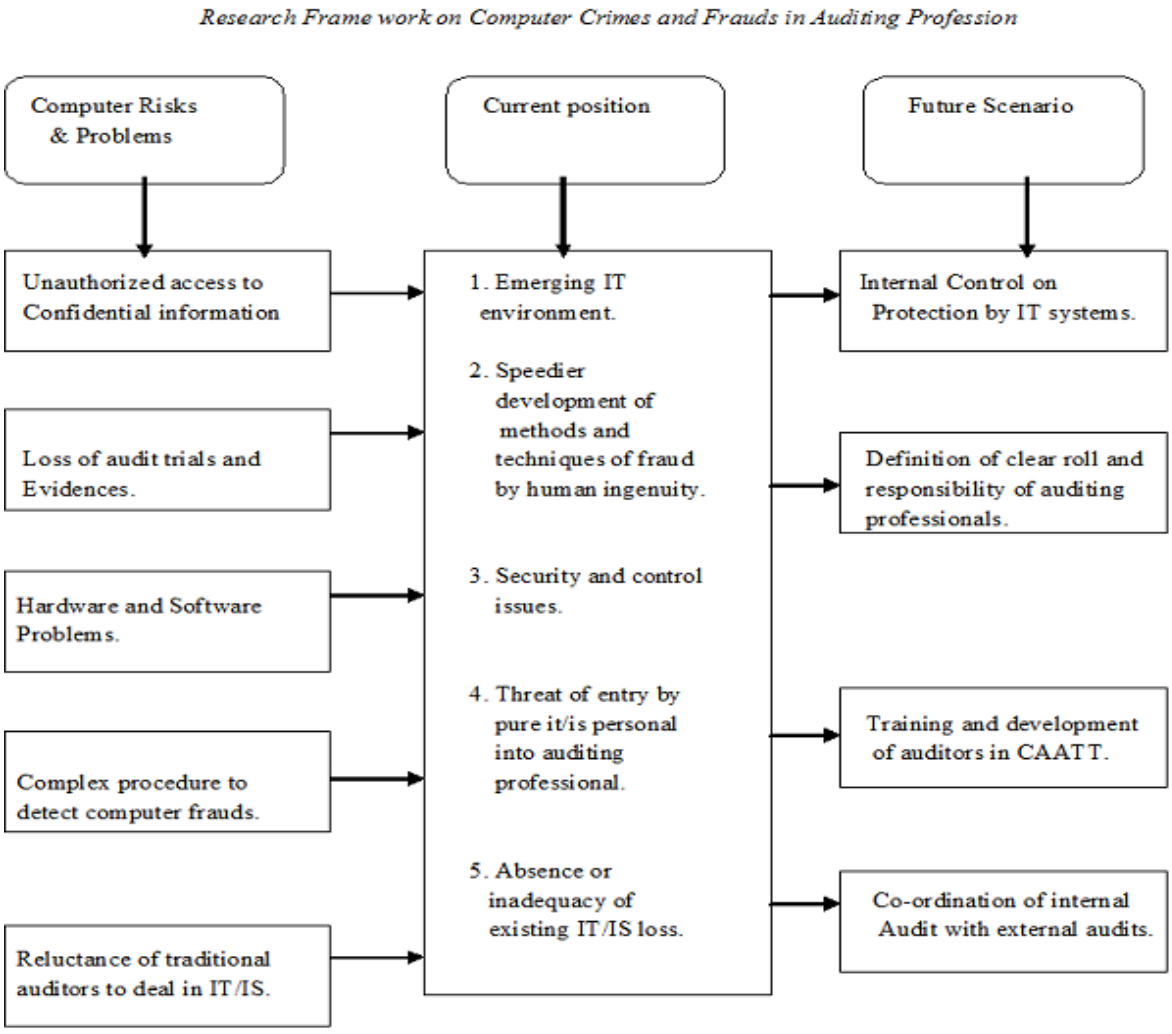

Figure 1: The research framework for discussion, analysis, and findings

4. Discussion

The migration of commercial and government applications to computers and the internet has caused a corresponding shift from the commission of crimes, traditionally focused on stealing physical assets, to the commission of crimes in cyberspace. Computer crime has only recently begun to receive the attention these invasive warrants. The shift of crime to intangibles and the crime committed by anonymous or pseudonymous individuals has a staggering impact on society, both socially and economically. Holt & Bossler (2008) emphasize using lifestyle-routine activities theory whereas Yar (2005) contested routine activity theory for cybercrime to understand such behavior. Maimon et al., (2013) identified that origin of computer-focused crimes against a large university computer network occurred during official business hours and origin was linked with users' countries of origin.

Computer Crimes are made possible by the combination of computers, digitized content, and telecommunications bandwidth. The power to send data over communications equipment has transformed our society completely this capacity to sent data, however, does not, operate in a

 ISSN 1927-033X

perfect world. Even when data send a criminal may be trying to steal or manipulate it, use it as ransom, spy on it, or copy it. Wori (2014) found that broad spread use of electronic medium has enhanced cyber crimes exponentially with severe lacking cross-border legislation to counteract cybercrimes.

The increasing dependence of business on computer system had made many more organizations vulnerable to the impact of computer crime. A company's size is a significant factor contributing to proper security policy implementation. Smaller businesses are less likely to have extensive security arrangements in place Kotulic and Clark, (2004). According to a study by Keller et al., (2005) one of the constraints of small businesses is that they lack adequate and diverse IT staff typical of larger companies. Also, many business managers in small enterprises have little understanding of IS threats and risks and their associated business implications Keller et al., (2005) Indeed, more companies are worldwide about the risk of Computer crime than they are about product liability, fraud, and theft. A recent survey of 2,000 UK public and private organizations showed a direct correlation between those industry groups that experience the most intrusions or another unauthorized user of the computer systems and those that had the highest level of technology use in the workplace. The banking and finance industries reported the highest incidence of computer misuse and also had one of the highest dependencies on the computer in the workplace. Compared to the primary and mining sectors that not only had the lowest level of misuse but also had the lowest penetration of computer of all the industry groups participating in the survey.

Computer fraud, on the other hand, presents an ever-changing landscape of opportunity for manipulation especially for the unhappy but trusted employee with knowledge of computer technology. Periodic audits may not be enough to contain this type of fraud. Manipulation of data files is the most difficult to deal with as there are no outward signs or indicators that anything is amiss. A problem facing most organizations is that complete knowledge required for the investigation and prosecution of computer fraud. In the fast-paced and ever-changing world of information technology and computers, skilled fraud investigators are currently in short supply including forensic accountants. Research has shown that people are reluctant to give information on security for several reasons (CRS, 2004) the fear for the enterprise reputation is one: IT security officers fear to lose their jobs, and the respondents fear that criminals can utilize the information or findings of the survey. Some scientists, Kotulic and Clark, (2004) had to discontinue their projects on IS due to a general lack of answers.

Changes in societies, markets, customers, competition and technology around the globe will force an organization to clarify their values and develop new operating strategic. Auditors have to recognize this strategic challenge for is auditors is to contribute practical solutions to those complex IT problems in a meaningful and objective manner which enhance respect for the audit function. When performing an audit, auditors should ascertain it meets the main purpose.Detail knowledge and understanding are necessary to expose and use digital evidence effectively in any information security investigation (Casey, 2011)

These primary objectives include security provisions that protect a computer system and data from unauthorized, access, modifications, accurate and complete computer transaction processing, identify improper source data according to prescribed managerial policies, to detect and prevent financial misstatements and finally the confidentiality of computer data files. Some information

 ISSN 1927-033X

and data found for businesses that are frequently under the supervision of a national authority, such as for instance the financial businesses or those enterprises that come under the Security Act. Using such data and the information is not of the problem, but since different laws, regulations and supervision methodologies make it difficult to use for the comparative purpose the findings between different sectors (Bowen et al., 2006). Hence, there arise a need and essence computer crime surveys. Such initiatives will enable the ideas of security metrics for management (Kovacich &Halibozek, 2006) to be also utilized on a national level to produce measurement indicators for information security.

The role and responsibility of an auditor towards computer fraud and crimes are to meet the main objective of computer security provisions. Regarding meeting the objective of computer security provision, the auditor should first identify the types of security error and fraud faced by companies; these include intentional damage to the system assets, unauthorized access, and modification of programs, theft, and interruption of business activities. The auditor then has to develop a protection plan to control procedures to minimize security error and frauds, by restricting access, protecting against computer virus, encrypting data, implementing firewalls and backup process to recover the system from failure and disasters. Auditors also have to inspect and review the computer system audit procedure and test the control audit procedure by observing and examining test procedures. Finally, the auditor needs to apply the compensating controls of sound personal policies because if security controls are deficient, the organization will face substantial risks. Dhillon & Moores, (2001) suggests that various technical, procedural and normative controls should be put in place to prevent illegal and malicious acts from taking place.

Given that one of the biggest exposures organization faces is new technology, auditors must keep abreast with information system Development and understand the implications of those developments. One significant challenge for auditors is the examination of new technology applications for control and security issues. Auditors with computer security skills should perform a periodic review of the system or network security controls. Auditors also must possess a sound knowledge of the subject matter audited, and a requisite knowledge of information systems and computer technology to conduct continues audit. Auditors need to understand what audited and use the appropriate technologies to facilitate the audit and detecting computer fraud. Davis (2012) found that due to lack of training, personnel and equipment to investigate cyber crime, there is still slackness in the enforcement of laws. The leadership of governments and law enforcing agencies should recognize the urgent need for effective enforcement.

The audit profession must adhere closely to the guidelines provided by governing bodies such the SEC, AICPA, the Sarbanes – Oxley Act 2002 and Supreme Court findings to regain the public trust which had eroded recently. Computer crime is an inevitable happening in an information age, although computers are equipped with fraud detection techniques to assist auditors to identify fraudulent activity, it is not sufficient enough to prevent computer fraud. The existence of computer-assisted audit tools and techniques (CATTS) have a particular effect on computer fraud prevention, but it will not eradicate fraud totally as the ingenuity of human mind cannot be undermined by existing fraud detecting system. A better and challenging up to date system ought to be maintained internally by all organization to combat future crime war.

 ISSN 1927-033X

5. Limitations

Given the short research period and the limited amount of literature surveyed one of the shortcomings of this paper is that it does not completely detail out all types of computer crime or computer related crimes that affect Audit profession directly or indirectly. Only the major type of computer crimes is related to auditing profession was discussed in detail. The applicability and the effectiveness of auditor's current fraud detecting techniques and devices explored to a limited extent. Whether the auditor's current level of Fraud busting technology is effective to detect and prevent cyber crimes remains unanswered? Whether with current technology auditors will reduce the cost of fraud to the society and the world economics also uncertain? Chu, B., Holt, T. J., & Ahn, G. J. (2012) demonstrated that the key role of bots and malicious software to facilitate cyber crimes could trim by disrupting by botnets and the markets that facilitate the distribution of malware and hack tools.

6. Conclusion

Computers are used in different ways to commit crimes, ranging from fraud to espionage to terrorism. Fafinski (2013) opined that future regulation on computer misuse should go beyond criminal and civil laws as well as non-legal means of governance including Internet users and user-groups, Internet service providers, corporations, the police and other non-police organizations. Some individuals are committing crimes even with no intent to profit from their actions. Saini et al., (2015) observed that cyber-attacks were taken place knowingly or unknowingly. Attacks done knowingly are cyber crimes which severely impacted the socially in the form of economic disrupt, psychological disorder, a threat to national defense, etc. The Internet and network computer crime are the unfortunate results of crime migrating to the places where the assets are.

Federal, State, and International laws are regularly amended to keep up with the new and creative crimes being committed. Shukan, A., & Erdogan, Y. (2013) Concluded that the current legal regulations in the many countries are not sufficient, no matter how many laws Federal or state pass, the most anticrime strategy is one of self-protection, a strategy of securing one's digital assets. Auditor's individuals, businesses, and government must be vigilant in their efforts to secure information, computer, and networks against criminal activities. Patchin & Hinduja (2011) has cautioned that growing proportion of youth are susceptible to online interpersonal violence, aggression, and harassment via cyber bullying. Schools, social workers, and parents need to be aware of on cyber bullying identification; prevention and response Governments are also attempting international initiatives to suppress computer crimes. Johnston & Warkentin (2010) emphasized that insiders should be engaged in these activities by managers through the use of security education, training, and awareness (SETA) campaigns. Nations are becoming increasingly cooperative in sharing information and assisting in the prosecution of international cyber criminals. The government's need to address cyber criminals on both a national and international level is of critical importance at this time, yet questions about its tactics persist. Due to very insecure and unusable atmosphere in cyberspace, Peykanpour & Jalali (2016) feared that the entire world would be in trouble unless people and foreign governments fight together to stop cyber crimes to provide cyber security.

References:

Barbara D. Ritchey (1996), "Computer Crimes and how to prevent them," September-23-1996.

 ISSN 1927-033X

Barbara R. Farrell, Joseph R. Franco (1999), "The role of the auditor in the prevention and detection of Business fraud, SAS, No. 82.

Bilal Makkawi, Allen Schick (2003), "Are auditors sensitive enough to fraud? Management Auditing Journal", Vol. 18, Issue 6/7.

Bruce R. Gaumnitz and John C. Lere (2004) "Codes of Ethics with impact" The CPA Journal." May2004.

C. Richard Baker (1999), "An analysis of fraud on the internet," Research the internet, Electronic Networking Applications and Policy, Vol. 9, 5 Nov 1999.

Casey, E. (2011). Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet.

Chu, B., Holt, T. J., & Ahn, G. J. (2012). "Examining the creation, distribution, and function of malware on-line.

Chula G. King and W. Timothy O'Keefe (2004), – "Online Identify Theft and business," CPA Journal, http://w.w.w.nysscpa.org.

David Thompson (1997), "Computer Crime and Security Survey," Information Management & Computer Security, Vol. 6, Issue 2.

Davis, J. T. (2012). "Examining perceptions of local law enforcement in the fight against crimes with a cyber component. Policing: An International Journal of Police Strategies & Management, 35(2), 272-284.

Dhillon, G., & Moores, S. (2001). Computer crimes: theorizing about the enemy within. Computers & Security, 20(8), 715-723.

Dorothy E. Denning (1990), "Concerning Hackers Who Break into Computer Systems," October-4-1990 http://w.w.w.sgrm.com./art.7.htm.

Edwin J. Kligmen (2003), "The need for old- Fashioned Ethics," The CPA Journal, December 2003.

Fafinski, S. (2013). Computer Misuse: Response, regulation, and the law. Routledge.

Gordon, L.A., Loeb, M.P. and Lucyshyn, W. (2003) 'Sharing information on computer systems security: An economic analysis,' Journal of Accounting and Public Policy, 22(6), pp. 461–485. doi: 10.1016/j.jaccpubpol.2003.09.001.

Holt, T. J., & Bossler, A. M. (2008). "Examining the applicability of lifestyle-routine activities theory for cybercrime victimization. Deviant Behavior, 30(1), 1-25.

Holt, T. J., & Bossler, A. M. (2012). Police perceptions of computer crimes in two southeastern cities: An examination from the viewpoint of patrol officers. American Journal of Criminal Justice, 37(3), 396-412.

Holt, T.J., and Bossler, A.M. (2013) 'Examining the relationship between routine activities and Malware infection indicators,' Journal of Contemporary Criminal Justice, 29(4), pp. 420–436. doi: 10.1177/1043986213507401.

Holt, T.J., and Turner, M.G. (2012) 'Examining risks and protective factors of on-line identity theft,' Deviant Behavior, 33(4), pp. 308–323. doi: 10.1080/01639625.2011.584050.

 ISSN 1927-033X

Hubert D. Glover, June Y. Aono (1995) "Changing the model for the prevention and detection of fraud" Managerial Auditing Journal, Vol. 10, No. 5.

James L. Bierstaker, Priscillia Burnaby, Jay Thibodeau(2001), "The impact of information technology on the audit process: an assessment of state of the art and implications for the future," Managerial Auditing Journal, Vol. 16, Issue 3.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: an empirical study. MIS Quarterly, 549-566

Keller, S., Powell, A., Horstmann, B., Predmore, C. and Crawford, M. (2005) 'Information security threats and practices in small businesses', Information Systems Management, 22(2), pp. 7–19. doi: 10.1201/1078/45099.22.2.20050301/87273.2.

Kotulic, A.G. and Clark, J.G. (2004) 'Why there aren't more information security research studies,' Information & Management, 41(5), pp. 597–607. doi: 10.1016/j.im.2003.08.001.

Maimon, D., Kamerdze, A., Cukier, M., & Sobesto, B. (2013). Daily trends and origin of computer-focused crimes against a large university computer network an application of the routine activities and lifestyle Perspective. British Journal of Criminology, azs067.

Narayanan, A. S., & Ashik, M. M. (2012). Computer Forensic First Responder Tools. In Advances in Mobile Network, Communication and its Applications (MNCAPPS), 2012 International Conference on (pp. 156-159). IEEE.

Patchin, J. W., & Hinduja, S. (2011). Cyberbullying Prevention and Response: Expert Perspectives.

Paul M. Clikeman(2003), "Education for the public trust," CPA Journal, August 2003.

Peykanpour, N., & Jalali, F. (2016). Computer Crime, Strategies and the Ways to Deal with them. European Online Journal of Natural and Social Sciences: Proceedings, 5(3 (s)), pp-67.

S. Keller, A. Powell, B. Horstman, C. Predmore and M. Crawford, Information security threats and practices in small businesses, Information Systems Management 22(2) (2005), 7–19.

Saini, H., Rao, Y. S., & Panda, T. C. (2012). Cyber-crimes and their impacts: A review. International Journal of Engineering Research and Applications, 2(2), 202-209.

Saini.H. et al. (2015) observed that cyber-attacks were taken place knowingly or unknowingly. Attacks done knowingly are cyber crimes which seriously impacted the socially in the form of economic disrupt, psychological disorder, a threat to national defense, etc.

Saini.H. et al. (2015) Restriction or prevention of such threats depended upon a proper analysis of attacker's behavior and understanding of the impacts.

Selvaraja D. Susela(1999), "Interest" and Accounting Standard Setting in Malaysia", –Accounting Auditing & Accountability Journal, Vol.12, November 3, 1999.

Shukan, A., & Erdogan, Y. (2013). Criminal Law Problems of IT-Crimes in Kazakhstan and Turkey. Middle-East Journal of Scientific Research, 17(12), 1752-1755.

Siew Kien Sia (2000) – "Surfacing the career development issue of is auditors the myths and the reality," Information system audit and control Association Info bytes.

Straub, D. W. (2009). Black hat, white hat studies in information security. Keynote Presentation of the 1st IFIP, 8.

 ISSN 1927-033X

Susan Haugen, J. Roger Selin (1999) - "Identifying and controlling computer crime and employee fraud," Industrial Management & Data Systems, Vol. 99, No. 8.

Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2014). Digital crime and digital terrorism. Prentice Hall Press.

Taylor, R.E., Fritsch, E.J. and Liederbach, J.C. (2014) Digital crime and digital terrorism (3rd edition). Available at: https://www.amazon.com/Digital-Crime-Terrorism-3rd/dp/0133458903 (Accessed: 11 August 2016).

Thomson, K.-L. And von Solms, R. (2006) 'Towards information security and competence maturity model,' Computer Fraud & Security, 2006(5), pp. 11–15. doi: 10.1016/s1361-3723(06)70356-6.

U.S Department of Labor Bureau of Labor Statistics, "Account and Audit," www.bls.gov

Vasiliy Polivanjuk (2000) – Computer Crime Research Centre (CCRC), http://crime – research.org/eg/library.

Warwick T. M. Peters (1997), a Further study in white collar crime: Hacking & Criminal Hacking – Computer, Crime Kevin Mitnick – regulation and control of white-collar computer crime.

Whitman, M.E. (2004a) 'In defense of the realm: Understanding the threats to information security,' International Journal of Information Management, 24(1), pp. 43–57. doi: 10.1016/j.ijinfomgt.2003.12.003.

Whitman, M.E. (2004b) 'In defense of the realm: Understanding the threats to information security,' International Journal of Information Management, 24(1), pp. 43–57. doi: 10.1016/j.ijinfomgt.2003.12.003.

Willison, R., & Warkentin, M. (2012). Beyond deterrence: an expanded view of employee computer abuse. MIS Quarterly, 37(1), 1-20.

Wori, O. (2014). Computer crimes: factors of cybercriminal activities. International Journal of Advanced Computer Science and Information Technology, 3(1), pp-51.

Rezaee, Z. (2004). "Restoring public trust in the accounting profession by developing anti-fraud education, programs, and auditing. Managerial Auditing Journal, 19(1), 134-148.

Yar, M. (2005). Computer hacking: Just another case of juvenile delinquency? The Howard Journal of Criminal Justice, 44(4), 387-399.

 ISSN 1927-033X