The Effect of Computer Crimes on the Application of Information System in Banks in Jordanian Firms

Mohammad Al-Tarawneh
Karak University College, Balqa Applied University, Salt, Jordan
E-mail:moh_8877@yahoo.com

Haroon Al-tarawneh
Karak University College, Balqa Applied University, Salt, Jordan
E-mail:haroontarawneh@yahoo.com

Mohammad Ma'aitah
Amman University College, Balqa Applied University, Salt, Jordan
E-mail:Z_maytah@yahoo.com

Abstract

This study aims to identify the effect of computer crimes on the application of information system in bank sector in Jordan. The study relied on both data resources; the primary and the secondary data were collected from a previous studies related to the subject matter, where as the primary data attained through distributing the questionnaire on the study sample.

The researchers conducted a statistical analysis for approximately 300 questionnaires , which were distributed on a sample of Jordan commercial banks, then the responses of the study sample were emptied into the computer, the data analysis was conducted by using statistical analysis system(SPSS), the result showed:

- There is a relation that has a moral effect between the dangers of viruses and efficiency of the information systems.
- There is a relation that has a moral effect between the dangers of penetration/violation and the efficiency of information systems.
- There is a relation that has a moral effect between losing and smuggling of information and the efficiency of information systems.

In light of the previous results, the researchers suggest a group of recommendations:

The researchers recommend the increase of research related to computer crimes, since it is clear from this study that there is a big gap in studies related to this approach. To publish statistics linked to the internet crimes and its misuse by concerned parties to identify the size of the problem. To form specialized committees of experienced figures to set special laws regarding the computer and the internet crimes in a detailed fashion of laws and regulations in an efficient way in Jordanian judicial authorities.

Keywords: Computer Crimes, Viruses, Penetration/Violation, Administrative Information System.

1. Introduction

The computer crimes are considered a new criminal phenomenon which started its way through the personal and the public life in all domains.

In this regard, we will demonstrate a set of statistics discussed by several research and studies represented in the information revolution as a human, economic and social phenomenon… which is unable to develop without the legal regulations that organize it use. The information systems become essential for all public and private business organizations as well as institution, government, departments, the importance of constant development in the human thought on the one hand and the development and advancement of technology on the other.

Hence, the study based on the identification of computer crimes effect on the application of information systems, it is hoped to provide a useful feedback to all whom it may concern in this topic.

2. Background

Criminal investigation is considered as a major topic of study for academics and practitioners. Brown in 2001 defined criminal investigation as "the process of legally gathering evidence of a crime that has been or is being committed". It looks for identifying the truths that are linked to how and why a crime took place, and works toward building a case that lead to the successful prosecution for the offenders.

The most important outcome of this investigation must be done by both detectives and patrol officers equally and should contribute equally to solve the cases, and it was UN helpful to put emphasis on one over the other (Eck, 1983). According to the research individuals in both positions should be less dependent on information supplied by the victims and more proactive in exploring leads provided by others related to the incident (Eck,1983). Eck pointed out that the most important techniques to increase the effectiveness of investigation are the practice of neighborhood canvassing and the use of informants. It obviously appeared that most information came from the victims of the crime at the beginning of the police response, much of those leads were worthless. If other sources were consulted, much more helpful information would be discovered. Eck also asserted the relative uselessness of re-interviewing the victim as one of the most practical recommendations to stem. Eck's study concerned to put these cases into categories included three groups, one of them, cases that could be solved, another one, those that have been solved, the other one, those that may be solved through some effort (Brown, 2001). This is called "the triage system". It was devised to help law enforcement personal in making decisions that are not influenced by personal opinions as to which cases were worthy of resource expenditure. Through this form of case screening. Investigations could go on in a targeted and informed manner after determining the presence of certain solvability factors that would likely lead to a case clearance. Wolfgang, Figlio, & Sellin, in 1972 stated that the triage system procedure also allowed law enforcement to tailor their efforts toward the small group of habitual offenders or 'career criminal' who commit the majority of serious crimes. Eck felt that these recommended changes would go a long way in refining the process and improving it usefulness and success rate. Royal Canadian Mounted Police in 2000 defined computer crime as "any illegal act fostered or facilitated by a computer, whether the computer is an object of a crime, an instrument used to commit a crime, or a repository of evidence related to a crime".

Some of the most important types include E-commerce fraud, child pornography trafficking, software piracy, and network security breaches. According to Leibowitz, 1999; United Nations, 1994; Wittes, 1994 investigative difficulties are introduced when attempting to deal with computer crimes because of its generally technologically-advanced nature, the fact that can occur almost directly, and because of being extremely difficult to observe, detector track.

Lyman in 2002 pointed out that these problems are compounded by the relative anonymity afforded by internet as well as the transcendence of geographical and physical limitations in cyberspace both of which render difficult the detection of criminals who are able to take advantage of a virtually limitless pool of victims. Money laundering with the use of computers concerns the process of concealing the source of illegally-obtained money and often involves the creation, fabrication, or alteration of documents to create a legitimate paper trail and history. Furthermore, Rosoff et al. in 2002 pointed out that witness in computer crime are relatively rare since these offenses tend to occur behind close doors.

According to Lyman in 2002, the only witnesses in most cases are those who commit the crimes either individuals or in groups, in addition to other techniques to gather information must be utilized.

Lyman and Rossf stated on interviewing as a tool that may provide indirect utility for the investigator, such as insight into the motives and possibly the specific techniques employed, particularly if the offender was an 'insider.' Motive for a crime such as embezzlement (the siphoning off of funds from an employer by an employee – often through the use of computer systems. Coleman and Ramos in 1998 asserted that motives for a crime might stem from organizational variables such as pressure from supervisors or managers to demonstrate productivity or effectiveness, or from a 'culture of competition' that permeates the enterprise.

Krause in 2002 pointed out that motive for a crime might stem individual-level variables such as a personality characterized by laziness, vengeful inclinations, a tendency to mock authority, or an inability to deal with stress in a pro-social manner.

Eck stated that the collection and use of physical evidence has been documented as vital and while this procedure in investigating computer crime is very time-intensive, it often yields key clues that can lead to an apprehension.

According to Lyman in 2002 and Webster in 1980 the manner in which evidence is procured in computer crime cases remains a sizable challenge for law enforcement. Specific information related to the computer system requiring search and possible seizure must be detailed in the warrant in order to be approved, and also so that the prosecutor can counter any evidentiary challenges brought by the defense staff. Consistent investigative standards and protocols for computer crimes have not yet become firmly ensconced in most police departments, and this can lead to evidence being deemed inadmissible – evidence that otherwise might have led to a conviction.

New Jersey Attorney General Commission of Investigation in 2000 stated that as result of the relative newness of search warrant applications for computer crimes, some state designating individual judges to deal with these specialized request must not be confused by technical details associated with the investigation, but should understand the nuances of what is involved so that the court can make an informed decision. The goal is to clearly articulate probable cause that a crime has been committed, and that the items described in the warrant are related to that crime.

Cyber crime is little different to any other kind of crime; the defining difference between cyber crime and traditional crime is that cyber crime is committed with the use of a computer (Whether it be a Desktop PC or an ATM machine). Almost all the kinds of traditionally accepted crimes could be performed with the aid of a computer (Gordon, 2000). Crimes such as fraud and forgery are relatively easy to perform and occur very frequently however; crimes such as murder can also be attributed to cyber crime. For example: If a person broke into and damaged or affected the network that controls the lights and junctions of Railway tracks and two trains happened to collide killing twenty people, that could be construed as murder. Another (which studies have shown to be a fairly common) crime is Hacking. Hacking can be likened to espionage since the people hacking into systems are often just going in to have a look around (spying) without intending to do any damage to the system or its integrity (this is not always the case, some cases of hacking , usually called cracking also occurs). According to Long & Long, (1999) cracking can be quite malicious and causes sever damage to systems and data integrity) this crime can be performed or executed from within or external to the organization (Gordon, 2000). Further more Vatis (2001) indicates that cyber attacker are attracted to “High Value Targets”; he goes on to define high value targets as network infrastructures whose disruption would have a symbolic, financial, political, or tactical consequences. Palestinian group attacks on Israeli banking and financial institutions’ web sites are a warning for potential attacks on the U.S economy (Vatis, 2001).

3. Study Objectives

- To identify the phenomenon which in fact not new but up to date with enormous development of information technology (IT).
- To observe the specific of computer crimes and extent of their effect on information systems.
- To demonstrate the types and nature of computer crimes.
- To demonstrate the effect of computer crimes on information systems through examining the relation them.
- To report some of the crimes those occurred previously and have a direct effect on systems.

4. Study problem

The study problem is included in the wide spread of computer crimes and the electronic risks, the problem can summarize by the following questions:

- Do computer crimes affect the application of information system in banks?
- Do banks in Jordan vulnerable for computer crimes such as penetration, threats and viruses?
- Do these dangers affect the competency and efficiency of information system in the banks?

5. Study importance

The importance of this research is emerges from its demonstration for the impact of computer crimes on the administrative system. We selected this topic to identify a new phenomenon which received insufficient attention in research, the few studies that dealt directly with the wide spread risks in the recent time which lead to the sprawl of crimes.

6. Procedural Identifications

- Computer Crimes: "illegal conduct that leads to legal punishment, resulted from deliberate willingness of computer facts". It is a generic identification for some extent for all figures of the mechanic computer crimes whether the crimes occurred by the mechanical computer or upon it.
- Information System: "a comprehensive and coordinated combination of information sub-system that integrated together to form a wise image to transfer data into information through several approaches to increase the productivity.
- Viruses: "it is an equivalent to an applied program designed by the devastators to accomplish certain goals in computer system.

7. Study Hypothesis

- There is a moral effect relation between the viruses risk and efficiency of information systems.
- There is a moral effect relation between the risk of penetration and the efficiency of information systems.

- There is a moral effect relation between the loss and falsification of information and the efficiency of information systems.

8. Study Results

8.1 First domain:

The descriptive statistics was used to find out the mathematical means, the deviations of study questions were summarized in the following table.

Table (1)

The mathematical means and standard deviations of the items of the first domain

Statement	Mathematical Means	The means of the instrument measure	Standard Deviation
1- Viruses threat information on computer and lead to difficulty in the flow and use of information.	3.523	3	.927
2-Viruses considered as the initial and first danger of computer apparatus.	3.655	3	1.407
3- Viruses considered among the basic problems and challenges of the digital age.	3.600	3	.844
4- Viruses lead to the loss of confidence in technique especially in the internet because it is the fertile medium for the spread of these viruses.	3.610	3	.621
5- The danger of viruses is real threat for technique industry and development.	3.510	3	0.821
6- The internet is an effective and quick medium for viruses sprawl.	3.920	3	0.752
Total Sum	3.636	3	0.895

Table (1) shows that the general mean of the subjects' responses on the first domain (the viruses) reached (3.636) with the "agree degree", and that the means of the standard deviation was (0.895).

From table (7) we notice that the attitudes of the study sample were positive towards all questions, their means were greater than the means of the measurement instrument

Which was (3), the highest item felt by the study sample in this domain was item (6) which suggest: (the internet is an effective and quick medium for viruses sprawl), the mathematical mean of this item was (3.920), then the item (2) which suggests :(viruses are considered the basic and first danger on the computer) and its mathematical means was (3.655).

8.2 The Second Domain: Penetration/violation.

The descriptive statistics was used to find out the mathematical means and deviation of the study question, they were summarized as follows:

Table (2)

Mathematical means and standard deviations for the item of the second domain (the penetration/violation)

Statement	Mathematical Means	The means of the instrument measure	Standard Deviation
7- The strategically, cultural, economic, importance of information considers the patterns of violation on information a serious danger since the 'these threat the culture and economic structure of the state.	4.500	3	.508
8-Some computer crimes violate the private life or what is called the human privacy.	3.600	3	.770
9-The information is the direct target since the penetrate or hacker seeks to change or steel or eliminate certain information.	4.300	3	.542
10- The economic impacts of computer crimes as a result of penetration lead for losses of million dollars annually.	4.180	3	.532
Total Sum	4.145	3	0.588

Table (2) show that the general means of the subject responses on the second domain "penetration/violation" reached (4.145) with "agree response" , and that the means of standard deviation reached (0.588).

Moreover, we notice in table (8) that the attitudes of the study sample were positive towards all questions, the mathematical means were greater than the mean of the measure instrument (3), the highest item felt by the study sample in this domain was item (7) which emphasizes (the strategically, cultural, and economic importance of information considered the violation of information as serious risk as it threats the cultural and economic structure of the state, the mathematical mean of this item was (4.500), then the item (9) which suggest (information is the immediate target, since the hacker seeks to change, steel or delete certain information), the mean of this item was (4.300) .

8.3 The Third Domain: Information loss or smuggling

The statistical description was used to count the mathematical means and standard deviation of the study questions; they were summarized in the following table:

Table (3)

The mathematical means and standard deviation for the items of the third domain (information loss or smuggling).

Statement	Mathematical Means	The means of the instrument measure	Standard Deviation
11- Information smuggling causes damage and disserve for the welfare of the national security and native sovereignty within the framework of what is known as information was.	3.122	3	.922
12- Computer crimes are considered to be international or political cross-borders crimes through smuggling information.	3.695	3	1.400
13-Espionage, defalcation and embezzlement which may be committed by computer.	3.630	3	.811
14- There are many computer crimes centered in establishing programs for information smuggling.	3.621	3	.655
Total Sum	3.517	3	0.947

Table (3) show the general of responses of the study sample subject on the theard domain "the loss and smuggling information" which reached (3.517) with the "agree response", and that the mean of standard deviation was (0.947)

From table (3) we notice that the altitudes of the study sample were positive toward all question, the means were greater than the mean of the instrument measure (3), and the highest item felt by the study sample in this domain is item (12) which says: " computer crimes are consider international or political cross-borders through smuggling information), in which means reached (3.695), followed by item (13) which suggests (espionage, and embezzlement may be committed by computer) since the mathematical mean was (3.630).

8.4 The Fourth Domain: Information System

The descriptive statistics were used to find out the means and standard deviation for the study questions which are summarized in the following table:

Table (4)

Mathematical means and standard deviations of the fourth domain (information system

Statement	Mathematical Means	The means of the instrument measure	Standard Deviation
15-Softwares used in information system are the best and the most recent available ones.	4.322	3	.922
16-The used software's allow to retrieve data and information when needed.	3.598	3	1.45

17-It is possible to modify the exited programs easily or to develop them or correct.	3.640	3	.866
18-The used programs provide information that assist in sitting future plans.	3.321	3	.632
19-Information system has a high ability to response for changeable conditions and new developments.	3.214	3	0.454
Total Sum	3.619	3	0.8648

Table (4) shows that the general mean of responses of the study sample subjects on the fourth domain " Administration Information System A.I.S) reached (3.619) with "agree response", and that the mean of the standard deviation was (0.8648).

From table (4) we notice that the attitudes of the study sample were positively correlated with all question, the means were greater than the mean of the instrument measure mean which was (3). The highest item felt by the study sample in this domain was item (15) which suggest: (the software used in recent the administrative system are the best and the most recent of the available), since the mathematical mean reached (4.322), followed by item (17) which say (the available programs can be modified easily, developed or corrected), the mean of this item was (3.640).

8.5 The Mathematical Mean and Standard Deviation for each Domain

The mean of each domain was counted to deal with each domain as one separated unit, the following are the means and standard deviations of the four study domains of the study subject (in table(11)).

Table(5)

Mathematical means and standard deviations of the study four domains of the study topic

Study Domain	Mathematical Means	Standard Deviation
First domain: Virus	3.636	0.895
Second domain: Penetration	4.145	0.588
Third domain: Loss and information smuggling	3.157	0.947
Fourth domain: Administrative Information Systems	3.619	0.864
Total	3.639	0.823

To acknowledge the relation between domains and the study subject Pearson's coefficient was used.

Table (6)

The values of Pearson's coefficients among the study subject and their evidence level.

Study Domain	Mathematical Means	Standard Deviation
First domain: Virus	0.521	0.000
Second domain: Penetration/violation	0.411	0.001
Third domain: Loss and information smuggling	0.121	0.002
Fourth domain: Administrative Information Systems	0.422	0.001

*(significant statistical evidence at level (ɑ̣≤.05)

Table (6) shows appositive significant statistical correlation at the evidence level (ɑ̣≤.05) of the study domains.

9. Study Hypothesis Test

It includes examining each of the study hypotheses.

9.1 First Hypothesis:

H0: there is no significant relation of moral effect between the viruses' risks and the efficiency of information system.

Ha: there is a significant relation of moral effect between the viruses' risks and the efficiency of information systems.

Table (7)

The result of Multiple Regression Analysis

The counted F	The tabulated F	Evidence level SIG	R	R^2	The result of the null Hypothesis
3.24	0.78	0.000	0.357	0.128	Refusal

To identify the extent of the affirmation and acceptance of this hypothesis, the two researchers tabulated value, and in accordance with the decision rule :the hypothesis (Ho) is accepted if the counted value is less than the tabulated value, also the rule of the decision says; the alternative hypothesis is accepted if the evidence level (SIG) is greater than (0.05), and the nihilistic Hypothesis is refused if the evidence level is less than (0.05), and through the above table, it is clear that the evidence level (SIG) equals (0.01) and since this evidence level is less than (0.05), then the decision rule suggests that there is a relation with a strong moral effect between the risks of penetration and the efficiency of information systems.

9.2 Second hypothesis

H0: there is no significant relation of moral effect between the risk of penetration and the efficiency of information systems

Ha: there is a significant relation of moral effect between the risk of penetration and the efficiency of information systems

Table (8)

The result of Multiple Regression Analysis

The counted F	The tabulated F	Evidence level SIG	R	R^2	The result of the null Hypothesis
3.247	0.78	0.032	0.387	0.058	Refusal

9.3 Third Hypothesis

H0: there is no relation of a strong moral effect between the information loss and smuggling of information and the systems.

Ha: there is relation of a strong moral effect between the loss and smuggling of information and the systems.

In order to acknowledge the extent of probability and acceptance of this hypothesis, the two researchers carried out the multiple regression analysis, and table (8) demonstrates this.

Table (9)

The results of the multiple regression analysis

The counted F	The tabulated F	Evidence level SIG	R	R^2	The result of the null Hypothesis
3.20	0.452	0.02	0.21	0.044	Refusal

The data reported in table (9) show that the value of (the counted F = 3.20) which is higher than its tabulated value, and in accordance with the decision rule: the hypothesis (Ho) is accepted if the calculated value is less than the tabulated value, also the decision rule emphasizes the acceptance of the alterative hypothesis if the evidence level (SIG) is greater than (0.05), the null-hypothesis is refused if the evidence level is below (0.05), and through the previous table, it is clear that the evidence level (SIG) equals (0.02), and since this evidence level is lesser than (0.05), then the decision rule suggests that there is a strong moral effect relation between the information loss and smuggling and the efficiency of information system.

10. Recommendations:

Through the previous results, the researchers could prescribe a group of recommendations included in the following:

1. The researcher recommends increasing the research related to computer crimes, since it is clear that there is a huge gap in the previous studies regarding this aspect.
2. Publish the statistics related to the computer crimes and computer abuse, by the concerned parties to identify the size of the problem.
3. The formation of specialized committees of experienced specialists to enact private lows correlated with the computer and internet crimes, and to put these laws and regulations into effect.
4. Spreading the system rights amongst various proxies was a lesson learned as the hacker used single login to hack into the entire system.
5. Continuous training is required for the business clients in order to share the responsibility in a fight against cyber crime.

6. As indicated above, as the technology advances, so is the rate cyber crime, subsequently new cyber laws should emerge to counter attack rapid changes.
7. Reactive and proactive security measure should run in parallel in the cyberspace to strike a balance in fight against cyber crime.
8. There should be a continuous research and development in IT security.
9. Since the institutions vary, it is important to ensure the relevance of the security measures that are to be adopted depending on the line of business and common type of cyber attacks.
10. The necessity to select the qualified and experienced professionals to carry out or execute the duties in an infinite accuracy.
11. The urgency to rehabilitate and train employees in the Jordanian banks in the field of information Technology (IT).
12. To promote the level of experience in the employees who work in the Jordanian banks through working on increasing scientific and practical awareness among them in the mechanical computer and the internet.
13. To conduct other similar studies for this study and to deal with other variables.
14. It is crucial to promote the systems, laws and legislations within the Jordanian kingdom to cope with the technological development, and to enact these laws, train judges and lawyers on these laws and regulations.

References

Brown, M. F. (2001). Criminal investigation: law and practice (2nd ed.).

Boston: Butterworth-Heinemann.

Eck, J. (1983). Solving crimes: The investigation of burglary and robbery. Washington, DC: Police Executive Research Forum.

Wolfgang, M. E., Figlio, R. M., & Sellin, T. (1972). Delinquency in a birth

Cohort. Chicago: University of Chicago Press.

Royal Canadian Mounted Police. (2000). Computer crime, can it affect you?

http://www3.sk.sympatico.ca/rcmpccs/cpu-crim.html

Leibowitz, W. R. (1999). How law enforcement cracks cybercrimes. New York Law Journal, 5.

United Nations. (1994). International Review of Criminal Policy - United

Nations manual on the prevention and control of computer-related crime. http://www.ifs.univie.ac.at/~pr2gq1/rev4344.html

Wittes, B. (1994). Perils of policing the internet: Law enforcement lacks the tools needed to go after a new breed of online criminal. The Recorder. No. October 11.

Lyman, M. D. (2002). Criminal investigation: the art and the science (3rd ed.). Upper Saddle River, N.J.: Prentice Hall.

Rosoff, S. M., Pontell, H. M., & Tillman, R. (2002). Profit without honor: white-collar crime and the looting of America. Upper Saddle River, NJ: Prentice Hall.

Coleman, J. W., & Ramos, L. L. (1998). Subcultures and deviant behavior in the organizational context. Research in the Sociology of Organizations, 15,3-34.

Krause, M. S. (2002). Contemporary White Collar Crime Research: A Survey of Findings Relevant to Personnel Security Research and Practice. The Personnel Security Managers' Research Program.

http://www.navysecurity.navy.mil/White%20Collar%20Crime.pdf

Webster, W. H. (1980). An Examination of FBI Theory and Methodology

Regarding White-Collar Crime Investigation and Prevention. American Criminal Law Review, 17(3), 275-286.

New Jersey Attorney General Commission of Investigation. (2000). Computer crime: A joint report. State of New Jersey, Commission of Investigation and the Attorney General of New Jersey. Trenton, New Jersey. http://www.state.nj.us/sci/pdf/computer.pdf

Gordon, B Adv. (2002, August). Hacking, denial of service and the Electronic Communications and Transaction Act. Servamus

Long, L. & Long, N. (1999). Computers. New Jersey, USA: Prentice Hall. Vatis, M.A. (2001). Cyber attacks during the war on terrorism: A predictive analysis