Islamic University of Gaza
Deanery of Graduate Studies
Faculty of Commerce
Business Administration
Department

الجامعة الإسلامية – غزة
عمادة الدراسات العليا
كلية التجارة
قسم إدارة الأعمال

Effectiveness of Information Security Management at the Palestinian Information Technology Companies

مدى فعالية إدارة أمن المعلومات في شركات تكنولوجيا المعلومات في فلسطين

By
Alaiddin Mahmoud Tayeh

Supervisor
Dr. Issam Buhaisi

Dissertation
Presented in Partial Fulfillment of the Requirement for

The Degree in
Master of Business Administration

1429هـ - 2008م

بسم الله الرحمن الرحيم

الجامعة الإسلامية – غزة
The Islamic University - Gaza

عمادة الدراسات العليا
هاتف داخلي: 1150

الرقم Ref. ج س غ/35/
التاريخ Date 2008/04/01

نتيجة الحكم على أطروحة ماجستير

بناءً على موافقة عمادة الدراسات العليا بالجامعة الإسلامية بغزة على تشكيل لجنة الحكم على أطروحة الباحث/ **علاء الدين محمود تايه** لنيل درجة الماجستير في **كلية *التجارة*/ قسم إدارة الأعمال** وموضوعها:

"مدى فعالية إدارة أمن المعلومات في شركات تكنولوجيا المعلومات في فلسطين"

وبعد المناقشة العلنية التي تمت اليوم الأربعاء 03 ربيع آخر 1429هـ، الموافق 2008/04/09م الساعة الثانية عشرة ظهراً، اجتمعت لجنة الحكم على الأطروحة والمكونة من:

د. عصام البحيصي	**مشرفاً ورئيساً**	.....
أ.د. يوسف عاشور	**مناقشاً داخلياً**	.....
د. محمد حسين	**مناقشاً داخلياً**	.....

وبعد المداولة أوصت اللجنة بمنح الباحث درجة الماجستير في **كلية *التجارة*/ قسم إدارة الأعمال**.

واللجنة إذ تمنحه هذه الدرجة فإنها توصيه بتقوى الله ولزوم طاعته وأن يسخر علمه في خدمة دينه ووطنه.

والله ولي التوفيق ،،،

عميد الدراسات العليا

د. مازن إسماعيل هنية

بسم الله الرحمن الرحيم

"فَمن يعملْ مِثْقَالَ ذَرةٍ خَيرا يره"

صدق الله العظيم

الزلزلة (7)

Abstract

This study aimed to identify the extent of the effectiveness of Information Security Management in Palestinian Information Technology companies (Jerusalem, Westbank, and Gaza). To achieve this aim, the researcher investigated ten domains of information security management in forty one companies. The ten domains included the Information Security Policy, Organizational Security, Asset Classification and Control, Personnel Security, Physical and Environmental Security, Computer and Network Management, System Access Control, Systems Development and Maintenance, Business Continuity Planning, and Compliance.

In addition, the researcher studied the differences between the companies in applying Information Security Management due to Company history in Information Technology (IT) field, Operating systems, Staff Qualifications, Staff Experience Years, Company Main Working Field, and Yearly Security Budget.

The findings of the research showed that all domains except the Organizational Security were affecting the effectiveness of Information Security Management in Palestinian Information Technology companies.

Moreover, there are no differences between the information technology companies in applying the information security management due to the Company history in IT field, Operating systems, Staff Qualifications, Staff Experience Years, Company Main Working Field, and Yearly Security Budget.

ملخص الرسالة

هدفت هذه الدراسة للتعرف على مدى فعالية إدارة أمن المعلومات في شركات تكنولوجيا المعلومات الفلسطينية (القدس والضفة الغربية وقطاع غزة). ولتحقيق ذلك الهدف قام الباحث بدراسة عشرة مجالات خاصة بإدارة أمن المعلومات في تلك الشركات. والعشرة مجالات هي سياسة أمن المعلومات، الأمن التنظيمي، تصنيف الأصول (الممتلكات) وضبطها، الأفراد وأمن المعلومات، الأمن المكاني، إدارة الشبكة والحواسيب، ضبط الوصول للأنظمة، تطوير وصيانة الأنظمة، تخطيط استمرارية العمل، و الامتثال للمتطلبات القانونية.

قام الباحث أيضا بدراسة الفروق بين الشركات تجاه تطبيقها لإدارة أمن المعلومات من حيث عمر الشركة في مجال تكنولوجيا المعلومات، أنظمة التشغيل المستخدمة، مؤهلات الأفراد، سنوات الخبرة لدى الأفراد، مجال العمل الرئيسي للشركة، و موازنة الأمن السنوية.

وقد توصلت الرسالة إلى أن جميع مجالات أمن المعلومات قيد الدراسة باستثناء الأمن التنظيمي تؤثر على فعالية إدارة أمن المعلومات في شركات تكنولوجيا المعلومات الفلسطينية.
وتوصلت الرسالة أيضا إلى أنه لا يوجد فروق بين شركات تكنولوجيا المعلومات الفلسطينية في تطبيق إدارة أمن المعلومات من حيث عمر الشركة في مجال تكنولوجيا المعلومات وأنظمة التشغيل المستخدمة ومؤهلات الأفراد وسنوات الخبرة لدى الأفراد ومجال العمل الرئيسي للشركة وموازنة الأمن السنوية.

Dedication

I dedicate this work to my mother, to my father who provided us with all needs to success, to my sons “Hazem and Obaida”, to my daughter Wafa, and to my wife Safa for her not ended patience and support.

Acknowledgments

I would like to thank Dr. Issam Buhaisi for his endless intellectual support and encouragement throughout the period of his supervision on this dissertation. Without such kind support and supervision the emergence of this dissertation would have been next to impossible.

I would like also to thank the examiners of this study; Dr. Yousef Ashour and Dr. Mohammed Hussin for the valuable directions and notes.

I am also very thankful to Dr. Samir Safi for his great assistance in the statistical analysis of the questionnaire.

Finally, I would like to thank my colleagues in the M.B.A program for their encouragement and support, and also my work colleagues for their support.

Table of Contents

List of Tables

List of Figures

Abbreviations

ALE	Annual Loss Expectancy
ARO	Annualized Rate of Occurrence
BCP	Business Continuity Planning
BIA	Business Impact Assessment
CA	Certification Authority
CISSP	Certified Information System Security Professional
CPU	Central Processing Unit
CRF	Company Risk Factor
CRL	Certificate Revocation List
DAS	Data Access Statements
DBMS	Database Management System
DDOS	Distributed Denial-of-Service
DOS	Denial-of-Service
DRP	Disaster Recovery Planning
EDI	Electronic Data Interchange
EF	Exposure Factor
HVAC	Heating Ventilation and Air Conditioning
ID	Intrusion Detection
IDS	Intrusion Detection Systems
IMAP	Internet Message Access Protocol
IP	Internet Protocol
ISM	Information Security Management
ISO	International organization for the Standardization
IT	Information Technology
LAN	Local Area Network
NAS	Network Access Server
OSI	Open Systems Interconnection
PIN	Personal Identifier Number
PKI	Public Key Infrastructure

PLD	Programmable Logic Device
RA	Registration Authorities
RADIUS	Remote Authentication Dial-In User Service
RAM	Random Access Memory
ROM	Read Only Memory
ROSI	Return on Security Investment
SLE	Single Loss Expectancy
SMTP	Simple Mail Transfer Protocol
VPN	Virtual Private Network

Glossary of Terms

Annualized Rate of Occurrence

Annualized Rate of Occurrence characterizes, on an annualized basis, the frequency with which a threat is expected to occur

Availability

Availability is the assurance that a computer system is accessible by authorized users whenever needed.

Confidentiality

Confidentiality is the protection of information within systems so that unauthorized people, resources and processes cannot access that information

Database Management System

A Database Management System is a collection of applications that manage large and structured sets of persistent data

Exposure Factor

The Exposure Factor is the percentage of loss that a realized threat event would have on a specific asset.

Integrity

Integrity is the protection of system information or processes from intentional or accidental unauthorized changes

Risk Management

Risk Management means the process of identifying, analyzing and assessing, mitigating or transferring risk

Single Loss Expectancy

The single loss expectancy measures the specific impact or monetary of a single event

Threat

A threat is simply any event that, if realized, can cause damage to a system, and create a loss of confidentiality, availability, or integrity

Trojan horse

A Trojan horse is a code fragment that hides inside a program and performs a disguised function

Virus

A computer virus is a malicious program designed to damage network equipment, including stand-alone computers

Worms

Worms are programs that reproduce by copying themselves through computers on networks

Appendices

CHAPTER ONE: BACKGROUND CONTEXT

1.1 Introduction

In this chapter; six topics will be discussed, these topics are research problem, research hypothesis, research objectives, research importance, research method, and previous studies.

1.2 Research Problem

The last two decades was seen an increased orientation of organizations becoming information intensive. Businesses are increasingly relying on Information Technology (IT) for their continued existence.

The growth of powerful and inexpensive computing in the last two decades brought IT into homes and small businesses. Small businesses have been dramatically affected by this increase (Phukan and Dhillon, 2000)

"The increasing reliance of organizations on information systems connected to or extending over open data networks has established information security as a critical success factor for modern organizations" (Kokolakis and others, 2000, P:107).

By checking many resources in the internet; nothing found about this topic regarded to Arabic companies, thus the need to check the Information security situation in the Palestinian IT companies raised.

The research problem could be identified as follows: **"To what extent the Information Security Management in the Palestinian Information Technology Companies is effective."**

1.3 Research Hypothesis

Hypothesis 1: There is a significant effect for written Information Security Policy on the effectiveness of Information Security Management in Palestinian Information Technology companies.

Hypothesis 2: There is a significant effect for Organizational Security structure on the effectiveness of Information Security Management in Palestinian Information Technology companies.

Hypothesis 3: There is a significant effect for Asset Classification and Control on the effectiveness of Information Security Management in Palestinian Information Technology companies.

Hypothesis 4: There is a significant effect for applying Personnel Security on the effectiveness of Information Security Management in Palestinian Information Technology companies.

Hypothesis 5: There is a significant effect for applying Physical and Environmental Security on the effectiveness of Information Security Management in Palestinian Information Technology companies.

Hypothesis 6: There is a significant effect for Computer and Network Management on the effectiveness of Information Security Management in Palestinian Information Technology companies.

Hypothesis 7: There is a significant effect for System Access Control on the effectiveness of Information Security Management in Palestinian Information Technology companies.

Hypothesis 8: There is a significant effect for Systems Development and Maintenance on the effectiveness of Information Security Management in Palestinian Information Technology companies.

Hypothesis 9: There is a significant effect for Business Continuity Planning on the effectiveness of Information Security Management in Palestinian Information Technology companies.

Hypothesis 10: There is a significant effect for Compliance with legal requirements on the effectiveness of Information Security Management in Palestinian Information Technology companies.

Hypothesis 11: There are differences denoting a statistical significance between Palestinian Information Technology companies in applying the Information Security Management attributed to the following variables:

-Company age in IT field.

-Type of Operating Systems.

-Staff qualifications.

-Years of staff experience

-Company’s main working field

-Yearly security budget

1.4 Research Objectives

The research objectives can be identified as follows:

1-To identify to what extent the information technology companies in Palestine are having a written Information Security Management Policy.

2-To identify to what extent the information technology companies in Palestine are having an Information Security Management Organization.

3-To identify to what extent the information technology companies in Palestine are having their Assets Classified and Controlled.

4-To identify to what extent the information technology companies in Palestine are concerned in the Personnel Security.

5-To identify to what extent the information technology companies in Palestine are concerned in the Environmental and Physical Security.

6-To identify to what extent the information technology companies in Palestine are concerned in Computer and Network Security Management.

7-To identify to what extent the information technology companies in Palestine are concerned in System Access Control.

8-To identify to what extent the information technology companies in Palestine are concerned in Security in Systems Development and Maintenance.

9-To identify to what extent the information technology companies in Palestine are concerned in Business Continuity Planning.

10-To identify to what extent the information technology companies in Palestine are Compliant to the legal requirements.

11-To identify the differences that affect the Palestinian Information Technology Companies concern in applying Information Security Management.

1.5 Research Importance

Needless to say that Palestinian IT companies operates in a critical field for the Palestinian people and businesses, they are the primary party who provided people and organizations with the new IT hardware and software solutions, the information in these companies needs to be protected in order to continue providing others with needed solutions.

Thus, it will be useful to investigate the information security management situation in these companies and provide them with the results to work on enhancing their practice in this field; this research could be a start for them toward applying the international standards in this field.

Furthermore, the importance of this research arises from the lack of such researches in Palestinian IT sectors (as far as I know); so it could be considered original one. The research also could be a reference for future researchers concerned in this topic.

1.6 Research Method

The descriptive analytical quantitative technique was used in this research because it is suitable and widely used in analyzing such this topic.

In addition to the primary data, the secondary data used; which included books, thesis and dissertations, research papers, articles, Internet websites, and newspapers.

The following scale was used for paragraphs to collect the respondents' answers.

Table (1. 1): Paragraphs Answers Weights Scale

Scale	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
Degree	4	3	2	1	0

In order to compare the means of paragraphs and domains; the following scale was used:

Table (1. 2): Data Analysis Scale

Scale	Interpretation
Above 2 mean	Agree
2 Mean	Neutral
Less than 2 mean	Disagree

1.7 Previous studies

1.7.1 Gritzalis (2000):

The research paper titled “Distributed component software security issues on deploying a secure electronic marketplace” focused on the distributed software security on deploying a secure marketplace. The paper considered a number of distributed component architectures and their security features to support the underlying infrastructure of Secure Electronic Transactions. The paper considered Authentication and Electronic Payment, along with a number of Corporate and Business to Business services are likely to rely heavily on this infrastructure, in order to establish a secure electronic marketplace. The paper also briefly presented TINA, an architecture offering a range of solutions for the up-and-coming transactions involving digital merchandise.

After comparing the security issues in three major models in distributed component software; authors found that:

-There are a lot of security issues still to be examined in distributed component software systems.

-Vendors and individual organizations in the electronic marketplace should be expected to improve and implement robust security infrastructures, in order to provide real value for their customers.

1.7.2 Phukan (2000):

This research paper titled “Ethics and information technology use: a survey of US based SMEs” aimed to study the beliefs and attitudes of small- and medium- sized enterprises (SMEs) toward the ethical use of information technology (IT).

Authors used “ethics survey”' conducted in the USA to collect the data they need. Authors found:

-Even though IT has become an integral part of the US SMEs, there is a clear lack of awareness of basic ethical issues.

-The participants on this survey did not seem to understand the importance of their moral and ethical responsibilities in the use of IT.

-Many users pay little or no attention to the laws of software piracy and unauthorized system access.

1.7.3 Hutchinson (2001):

This exploratory research paper titled “Attitudes of Australian information system managers against online attackers” aimed to establish a general impression of the attitudes of Australian professionals in business and government to the concept of “cyber-vigilantism”. It was undertaken as an initial project to provide the context for a larger, formal international survey. Authors defined the Cyber-vigilantism as the proactive process of responding to information attacks by hackers with corresponding attacks on them. Authors added that, in short, it is hacking the hackers.

The research also, explored the policies and procedures which have been set in place by various organizations to cope with concerted attacks on their systems.

Authors found that although a majority of managers do approve of the concept of “striking back”; only a minority are prepared for this eventuality. Authors also added that there appears to be complacency about the threats posed by organized, offensive attackers.

1.7.4 White (2001):

This research paper titled “Controlling corporate e-mail, PC use and computer security” conducted by two researchers who inspired to conduct this study because the survey results, which is that corporations began to use computer technology before safeguards were in place regarding its use; and the majority of the company's safeguards continue to be lacking. Not having the control function in place has caused dire consequences for many companies; authors said.

The research was limited to control of personal use of computers, controlling e-mail accounts, and securing company data. Over 200 companies in the south USA were surveyed.

The authors found that:

-A better control in majority of companies is still needed.

-Company policies regarding personal use of computers are still needed.

-More monitoring to prevent suits in areas of harassment, libel, and race discrimination is still needed.

1.7.5 Gerber (2001):

This research paper titled “Formalizing information security requirements” aimed to illustrate that the effectiveness of risk analysis, as a technique used to determine the required level of information security, is no longer adequate to protect modern information resources any longer and to introduce a more modern approach, based on information security requirements. Authors argued that risk analysis, concentrating on assets, threats and vulnerabilities, used to play a major role in helping to identify the most effective set of security controls to protect information technology resources.

Authors also added; to successfully protect information, the security controls must not only protect the infrastructure, but also enforce certain security properties in the information resources. To accomplish this; authors said: a more modern top-down approach is called for today, where security requirements driven by business needs state the level of protection required.

Authors found a Security Requirements Exercise (SRE) to determine the security requirements which is based on two dimensions. The first dimension is required to consider all factors related to the amount of security necessary for each security concern. The second dimension is used to determine the impacts that unwanted events might have on organizational processes, products and services.

1.7.6 Chan (2001):

This research paper titled “Integrating security design into the software development process for e-commerce systems” the authors proposed a software development process for secured systems (SDPSS) based on unified modeling language (UML), in which security design is integrated and means are provided to check whether the security requirements have been incorporated into the final design.

Authors used a simplified supply-chain e-commerce system as an example; integration of security design into the software development process is shown with discussions of possible security assurance activities that can be performed on a design.

1.7.7 Janbandhu (2001):

This research paper titled “Novel biometric digital signature for Internet-based applications” aimed to introduces the notion of biometric signature – a new approach to integrate biometrics with public key infrastructure, using biometric based digital signature generation which is secure, effective, fast, convenient, non-invasive and correctly identifies the maker of a transaction.

Authors said that personal identification numbers, passwords, smart cards and digital certificates are some of the means employed for user authentication in various electronic commerce applications. Authors also added that, these means do not really identify a person, but only knowledge of some data or belonging of some determined object.

Author’s approach also suggests two schemes for biometric signature using two existing and widely used digital signature algorithms, RSA and DSA, and discusses the problems associated with them individually. Speed of both schemes (based on iris recognition) is measured and compared with the help of JAVA implementation for both approaches.

1.7.8 Loukis (2001):

This research paper titled “Information systems security in the Greek public sector” investigated a set of 53 Greek public sector organizations concerning important aspects of information systems security.

Authors stated that the security aspects of public sector information systems are important as the respective systems are often part of critical infrastructures or deal with personal or sensitive data.

Authors found that Greek public sector organizations have only a basic level of information system security awareness. And only a small percentage have developed a systematic, complete, and integrated approach towards the security of their information system, including internal audit procedures.

Authors found also that the importance of proper training and generally the importance of the human factor for achieving high levels of information systems security are often underestimated.

1.7.9 Ye (2001):

This research paper titled “Robust intrusion tolerance in information systems” discusses causes, chain effects and barriers of intrusions into information systems, and reveal roles that various information security techniques play in intrusion tolerance.

Authors said that intrusions exploit vulnerabilities and introduce external disturbances into information systems to compromise security attributes of information systems such as availability, integrity, and confidentiality.

Authors also added: Intrusions into information systems cause faults of software and hardware components in information systems, which then lead to errors and failures of system performance.

Authors concluded that intrusion tolerance requires information systems to function correctly in a timely manner even under impact of intrusions.

Authors presented two robust intrusion tolerance methods through fault masking: Taguchi's robust method for system configuration and sharing of resources via an information infrastructure for redundancy.

1.7.10 Lee (2002):

This research paper titled “A holistic model of computer abuse within organizations” in which the authors said that past studies suggest that computer security countermeasures such as security policies, systems, and awareness programs would be effective in preventing computer abuse in organizations. Authors also added: they are based on the general deterrence theory, which posits that when an organization implements countermeasures that threaten abusers, its computer abuse problems would be deterred.

Authors proposed a new model of computer abuse that extends the traditional model with the social criminology theories, they focused on computer abuse within organizations, and the model explains the phenomenon through social lenses such as social bonds and social learning.

Authors concluded that the new model contributes to our theoretical body of knowledge on computer abuse by providing a new angle for approaching the problem, and it suggests to practitioners that both technical and social solutions should be implemented to reduce the pervasive computer abuse problems.

1.7.11 Irakleous (2002):

This research paper titled “An experimental comparison of secret-based user authentication technologies” presents a comparative study of software-based user authentication technologies, contrasting the use of traditional password and personal identifier number (PIN) against alternative methods involving question and answer responses and graphical representation.

The authors said that all methods share the common basis of secret knowledge and rely upon the user’s ability to recall it in order to achieve authentication.

The authors described an experimental trial along with the results based upon 27 participants. They also assessed the alternative methods in terms of practical effectiveness, as well as the perceived levels of user friendliness and security that they provide.

Authors concluded that while passwords and PIN approaches garner good ratings on basis of their existing familiarity to participants, other methods based upon image recall and cognitive questions also achieved sufficiently positive results to suggest them as viable alternatives in certain context.

1.7.12 Maguire (2002):

This research paper titled “Identifying risks during information system development: managing the process” attempted to show that there are many areas of potential risk within the process of information system development (ISD) and these need to be carefully analyzed and managed. Author said that certain popular risk management methodologies do not reflect the risk elements identified within the ISD process.

Through the case study, the paper has shown that there is a need to develop a risk analysis methodology that incorporates the key issues that need to be addressed before a system goes live. Author added that with risk analysis; the elements of risk have to be isolated at early stage.

Author found some potential risk elements which extracted from the case study, some of these elements are multi-tasking capabilities, change several project managers for the development team, lack of rigorous testing, and number of stakeholders.

1.7.13 Seleznyov (2003):

This research paper titled “Using continuous user authentication to detect masqueraders” proposed an approach for continuous user authentication based on the user's behavior, aimed to develop an efficient and portable anomaly intrusion detection system. Authors said that a prototype of a host-based intrusion detection system was built, and it detected masqueraders by comparing the current user behavior with his/her stored behavioral model. Authors also added that the model itself is represented by a number of patterns that describe sequential and temporal behavioral regularities of the users.

Authors also discussed implementation issues, described the solutions and provided performance results of the prototype.

Authors found that there are temporal patterns in user behavior and they may be used as well as sequential ones to efficiently detect anomalies in user behavior. Authors also believed that the temporal may support the anomaly detection, significantly increasing the probability of correct classification.

Authors also proposed an efficient way to build and maintain user profiles, keeping resource consumption to a reasonable level.

1.7.14 Hong (2003):

This research paper titled “An Integrated system theory of information security management” aimed to build a comprehensive theory of information security management by trying to integrate security policy theory, risk management theory, control and auditing theory, management system theory and contingency theory.

Authors suggested that an integrated system theory is useful for understanding information security management, explaining information security management strategies, and predicting management outcomes. Authors also added that few information security strategies and guidelines could be found for practitioners which may result from a lack of coherent and comprehensive information security management theory.

Authors found a proposed theory that:

-Provides rich information security strategies, procedures and theories for researchers, information security decision makers, planners, providers and users; thereby they can get a better understanding of information security in terms of different perspectives.

-Explains organizational behavior regarding information security management, and provides alternatives for organizational security management strategies.
-Could be applied to predict the organizational attitudes and behavior towards information security management, and could be beneficial for information security decision making.
-Could be a building block for further information security management researcher and be a guidance of future empirical studies.

1.7.15 Tsoumas (2004):

This research paper titled “From risk analysis to effective security management: towards an automated approach” aimed to describe requirements for a software tool that could assist in the transition from high-level security requirements to a formal, well-defined policy language. Authors said that such a tool would provide valuable assistance and support in both policy implementation and overall security management.

Authors also added that one of the various outputs of a risk analysis is a set of recommended practices expressed in high-level statements of a natural language, and in order to be applied to the real world, it is necessary to technically implement those requirements tailored to the specific organizational context. This is usually performed by experienced individuals, authors added.

Authors proposed candidate architecture for a policy tool, demonstrating that its implementation is achievable. Authors also argued in this paper that there is a need for further assistance of the security expert’s work by automated tools; whether hers/his work can be fully automated is not an issue as such, but it is sure that any contribution eases the burden of the security management.

1.7.16 Luthy (2006):

This research paper titled “Laws and regulations affecting information management and frameworks for assessing compliance” aimed to consider a number of key laws and regulations that have implications for information management and internal control systems.

The paper is a discussion of the key laws and regulations. It also considered a number of frameworks that may be useful for assessing compliance with applicable laws and regulations.

The paper found that organizations worldwide are impacted by an increasing number of laws and regulations. Many of them have important implications for information management and internal control systems even though they may lack explicit references to information management. This is because information technology (IT) has become pervasive in modern organizations, and it is self evident that awareness of applicable laws and regulations, along with their potential impacts on information management systems is critical for compliance.

1.8 Previous studies discussion

After reviewing the previous studies, the following can be noticed:

-Vendors and individual organizations in the electronic marketplace should be expected to improve and implement robust security infrastructures, in order to provide real value for their customers.

-There is a clear lack of awareness of basic ethical issues in the use of IT.

-Many users pay little or no attention to the laws of software piracy and unauthorized system access.

-Architectures, processes, approaches, frameworks and theories were suggested in toward enhancing information security management.

But this study has investigated to what extent the Palestinian information technology companies are applying the ten domains of information security management.

CHAPTER TWO: THEORETICAL FRAMEWORK

2.1 Introduction

This chapter is divided into eleven sections, the first section contains this introduction, and the other ten sections introduce the ten domains of Information Security Management (ISM) as it was organized by the ISO 17799.

While he was surfing the Internet; the researcher noticed that the big Information Technology (IT) companies such as Microsoft, Sun, and Cisco spent increasing efforts in developing techniques, tools and documentations in order to offer information security solutions. The researcher also noticed that a lot of specialized companies had been established to introduce consulting services in ISM field.

As a growing field, the ISM took the concern of some specialized institutions, centers, and agencies. The security professional now can get certificates in this field; one of the most famous certificates is the Certified Information System Security Professional (CISSP). The importance of security certificates rose because of the increasing demand on security professionals by different businesses.

2.2 Information Security Management

Computers are becoming a basic component of everyday operations, and organizations depend on them. A failure in computer system could have a critical impact on the organization, so the potential vulnerabilities in a computer system that could challenge operations must be minimized or eliminated (Shim and others, 2000).

Information Security Management in an organization requires the organization to identify its information assets and implementing of policies, standards procedures and guidelines that insure the information availability, integrity and confidentiality (Hansche and others, 2004).

2.2.1 Elements of Computer Security

Computer security is based on eight major elements; and following are these eight elements (NIST, 1996):

1. Computer security should support the mission of the organization.
2. Computer security is an integral element of sound management.
3. Computer security should be cost-effective.
4. Computer security responsibilities and accountability should be made explicit.
5. System owners have computer security responsibilities outside their own organizations.
6. Computer security requires a comprehensive and integrated approach.
7. Computer security should be periodically reassessed.
8. Computer security is constrained by societal factors.

2.2.2 Purposes of Information Security Management

Information Security main purpose is to protect the valuable resources and assets of an organization, such resources could be information, hardware, and software.

The information security management is all about insuring three requirements of the company's information resources; such requirements are availability, integrity and confidentiality.

Many authors have identified these requirements:

-AVAILABILITY: "Availability is the assurance that a computer system is accessible by authorized users whenever needed."

-INTEGRITY: "Integrity is the protection of system information or processes from intentional or accidental unauthorized changes"

-CONFIDENTIALITY: "Confidentiality is the protection of information within systems so that unauthorized people, resources and processes cannot access that information" (Hansche and others, 2004, P:3-6)

2.2.3 Risk Analysis and Assessment

Organizations have three choices to choose from in order to deal with the risk if they assessed that they could be exposure to such risk One is to accept the risk as it is without

any actions. Second is to take some actions to mitigate the effect of that risk to an acceptable level. Third is to transfer that risk to a third part like insurance.

The Risk Management means the process of identifying, analyzing and assessing, mitigating or transferring risk. And there are four questions considered as a core of the Risk Management process which are:

1-What could happen, which means what is the expected threat or event?

2-If it happened, what its impact on the organization?

3-How many times it could happen in a certain period of time?

4-What is the probability of the answers of the previous three questions?

After answering the four questions, the management can convert these answers into numbers in order to deal with it as money wise after identifying the value of the assets that could be harmed; this could be done by answering the following three questions:

1-What can be done to mitigate the risk?

2-How much will it cost?

3-Is it cost effective? (Hansche and others, 2004, P: 8-9)

As shown in Figure(2.1) and according to 2007 Computer Crime and Security Survey (2007 CCSS) that held by Computer Security Institute (CSI) in the United States; 29% of respondents said Yes when they asked if they have external insurance policies to manage its cybersecurity risks; and 71% of them said No for that question. The survey was answered by 454 computer security practitioners in U.S. corporations, government agencies, financial institutions, medical institutions and universities.

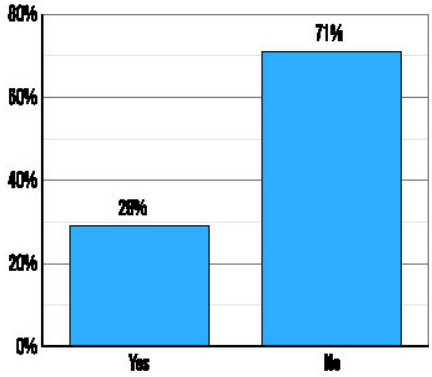


Figure (2. 1): Using External Insurance Policies to Manage Risks
Source: (2007 CCSS) http://www.gocsi.com, (Jan 2008)

"The ability of a corporation to identify risks and prevent incidents or exposures is a significant benefit to ensuring continued business viability and growth even in the midst of increasing threats and pressures" (Henry, 2004, P:1189).

In order to have a successful information security program; the organization needs an effective risk management process, and such process goal should be to protect the organization and all assets and facilities used to achieve its mission. And the risk management process is not a technical function only, but it should also be considered as a management function of the organization (Bowen and others, 2006).

2.2.4 Return on Security Investment (ROSI)

In this section, the basic methods of finding the ROSI for an organization and the implications that this will have on the business of security will be discussed. A seven-step analysis will be examined to help determine the ROI for security.

2007 CCSS rose that 39% of respondents said that they use ROI as a financial metric for quantifying the cost and benefit of computer security expending.

"Risk management is the careful balance between placing controls into the business processes and systems to prevent, detect, and correct potential incidents; and the requirement that the risk management solution not impede or restrict the proper flow and timeliness of the business" (Henry, 2004, P:1188).

The needed controls need money to be implemented, thus the expression Return on Security Investment ROSI raised, which requires the organization to balance between the loss value and the controls value, because it's none sense to implement controls costs you for example 100,000 Dollars to protect against a threat could cause a loss of 20,000 Dollars. So, the organization should calculate the ROSI before implementing any controls; and here we will discuss how to calculate the ROSI:

Following are the seven steps to calculating the ROSI:

Step One: Asset identification and valuation

The organization has to list its tangible and intangible assets and identify its values.

Step Two: Threat and vulnerability exposure factor

The Exposure Factor (EF) is the percentage of loss that a realized threat event would have on a specific asset. EF is from 0 up to 100, if the number is high, that means the loss is big, for example in the case of the fire in the servers room, the EF will be very high, if a hard disk lost the EF could be low.

Step Three: Determine the single loss expectancy (SLE)

The single loss expectancy (SLE) measures the specific impact or monetary of a single event. The following formula derives the SLE:

Asset Value X Exposure Factor = SLE

Step Four: Annualized rate of occurrence (ARO)

The annualized rate of occurrence (ARO) is the frequency with which a threat is expected to occur. The number is based on the severity of controls and the likelihood that someone will get past these controls. ARO values fall within the range from 0.0 (never) to a large number.

Step Five: Compute the annual loss expectancy (ALE)

The ALE can be computed by using the following formula:

ALE = SLE X ARO

After knowing the ALE, the information security management can determine the risk mitigation strategy they will use.

Step Six: Survey controls

You can now list the controls that applied in the place, and the SLE of each asset you have, if the SLE high, then a new controls needs to be implemented.

Step Seven: Calculate ROSI

The ROSI can be calculated by using the following formula:

ROSI = ALE – Current Cost of Control (CCC) (Endorf, 2004, P:1056-1057).

As shown in Figure (2.2) and according to (2007 CCSS); the average loss per respondent was 345 thousands of US dollars. The figure also shows the average of loss per respondent in the past eight years.

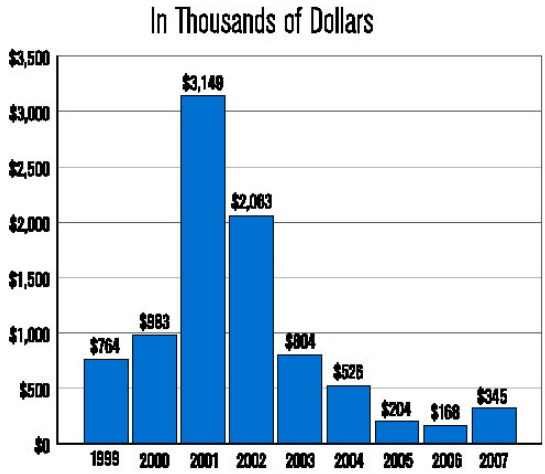


Figure (2. 2): Average Losses
Source: (2007 CCSS) http://www.gocsi.com, (Jan 2008)

They same survey also show the percent of losses due to insiders, Figure (2.3) shows those percentages.

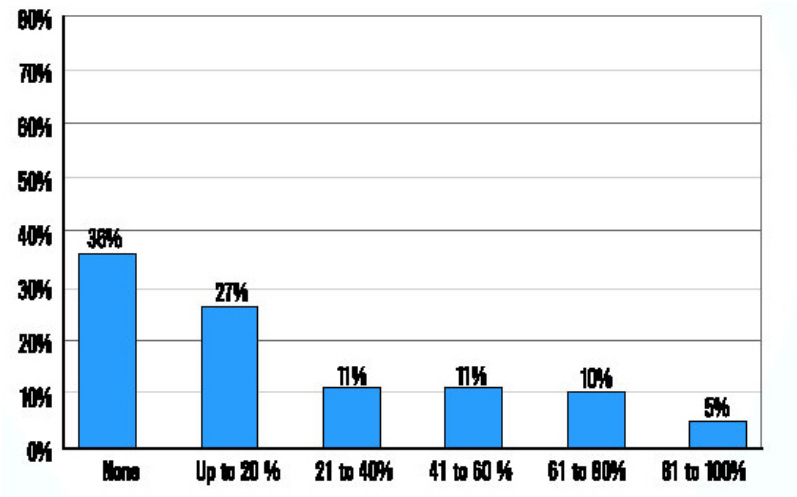


Figure (2. 3): Average Losses Due to Insiders
Source: (2007 CCSS) http://www.gocsi.com, (Jan 2008)

2.2.5 Security Policy

Information security policy as it was identified by (Bowen and others, 2006), is a collection of directives, rules, and practices that prescribes how an organization manages, protects, and distributes the information.

"The goal of the security policy is to translate, clarify and communicate management's position on security as defined in high-level security principles. The security policies act as a bridge between these management objectives and specific security requirements." (Weise and Martin, 2001, P: 3)

Policy should be short, constituted of series of clear and specific points, not more than one side of paper, because the shorter document is the more read one by employees.

Security policy should contain:

- Information security roles and responsibilities;
- Security controls baseline and rules of exceeding the baseline; and
- Rules of users' behavior and minimum consequences for noncompliance (Bowen and others, 2006).

2.2.5.1 Why firms need the security policy

The security policy is important for the following reasons:

First, it provides guidance for users, staff and managers for handling the firm's assets. Second, it forms the foundation of the control framework that will be applied. Third, it defines staff roles and responsibilities (Purser, 2004).

The security policy also defines what is allowed to access and to do, and what is not allowed to access and to do, and through this it protects the business (Maiwald and Sieglein, 2002).

2.2.5.2 The Types of Policies

This section shows the three types of policies as they are described by (Hare, 2004, P:1390-1391).

-Regulatory: Regulatory policies are security policies that the organization is required to implement, because it consists of some regulations or/and legal requirements imposed by the government bodies to organize some certain of professions like medicine and law.

-Advisory: Advisory policies are not mandated, but it’s strongly suggested to be followed in some events such as job warning and termination.

-Informative: Informative Policies are not mandate too, its purpose is to inform the individuals with some information, and no consequences on individuals if they are not follow or apply it.

2.2.5.3 Policy versus Procedures

Shorten (2004) argues that the policy defines and states what should be done, the author also added; but procedures tell how that thing should be done. For example, if the policy says, "All users must have a password", the procedure would tell more information about that password, in terms of its length, its lifetime, level of complexity...etc.

2.2.5.4 Content of the Security Policy

This section describes some issues that could be parts of the security policy, but it is not limited to such issues:

-Access Control Standards: Every user should be granted the only needed permissions that allow him/her to access the information systems and services that make him/her capable of doing his/her duties.

-Backups: The backup of the databases, users' files and software should be done in a regular basis, and the backup media should be kept in a secure place. The backup media will be used in case of failure or loss of data, and restore the corrupted or lost files and applications.

-Business Continuity Plans: Business Continuity Plan BCP should be developed, updated, and tested. Such plan will be used for all critical information systems and services to minimize the restore time of the business in case of failure.

-Physical Security: There should be a policy to protect the information facilities from physical side, such policy should make sure those information systems, removal storage media, electrical and communication services are well protected against unauthorized access as far as possible, these protection controls should be consistent with a cost-efficient operation.

-Viruses: The number of viruses is increased every day, it's very necessary for the organization to have an antivirus installed on all computers, but this not means that the staff members are not responsible in this manner, they should make sure that nay files should be checked before being loaded to the network, and they should report any detected viruses to the IT department in the organization.

-Noncompliance: The policy should also contain the actions that the organization may take if the staff member not compliance with the security policy, and the staff members should be noticed and know such actions.

-Legislation: The security practitioner should be conversant with the legislations that relevant to the aspect of information security, in order not to violate these legislations and put his/her organization in a critical situation (Shorten, 2004, P: 1375-1379).

2.2.5.5 Writing a Security Policy

-Draft and get acceptance: The security practitioner should first draft the policy, ask all interested parties to put their comments on it, make any changes on it and then submit it to the board for acceptance and sign-off by CEO.

-Distribute: After getting the acceptance on the policy, the policy practitioner should send it to all staff members to read it, and there should be a way to make sure that all of them have read it, for example, asks them to sign a document to approve that they read the policy (Hare, 2004).

2.2.5.6 Reviewing the Policy

The policy should be reviewed in a regular basis, and the period between two review processes depends on the volume of changes that could be happened in the working environment. Such changes could be a new technology, no more use for one technology, and a new way to use an existing technology. The changes in the policy could be to add, remove or update parts of the policy (Hare, 2004).

2.2.5.7 Staff Awareness

If you put a good policy, but your staff does not understand it, the policy will be useless. So, the staff members should be educated, and feeling that the policy will protect them (Hare, 2004).

2.3 Security Architecture

Five topics will be discussed under the Security Architecture section, such topics are Platform Architecture, Network Environment, Enterprise architecture, Security Models, and Protection Mechanisms.

2.3.1 Platform Architecture

In this topic, the computer and how it manages the systems resources and utilities are discussed. To explain this, the topic is separated into the following points:

- Operating System Software and Utilities
- Central Processing Unit (CPU) states
- Memory Management Overview
- Input/Output Devices
- Storage Devices

2.3.1.1 Operating System Software and Utilities

There are two primary objectives of the operating system; the first is to control the use of the system's resources which the operating system shared between the users and/or the tasks. The second objective is to present an easy to understand interface of the computer to users or programs.

The following terms are a associated with operating systems:

- *Multitasking:* Multitasking systems allows the computer to execute more than one computer task at the same time. The operating system keeps track with all these tasks without losing any information related to any one of these tasks.
- *Multithreading:* is the ability of the program to handle requests from more than one user in the same time; and to handle more than one request by the same user without having to have multiple copies of the software to be running.

- *Multiprogramming:* a multiprogramming system is the one that allows the execution of two or more programs by the same processor. Most of the operating systems nowadays are support multiprogramming.
- Multiprocessing: is the coordinated processing of two or more programs that running on a computer uses two or more processors. This feature allows the application to be executed by more than one processor in the same time to achieve a fasting processing of the programs.

Vulnerabilities of Operating Systems

Object reuse: The object reuse vulnerability is associated with multiprogramming systems. So, for security reasons; it is important to avoid storage residues. Storage residues occur when data is left in the memory area that could be used by new processes. A process returning Random Access Memory (RAM) to the operating system can clean the RAM before releasing it. The operating system itself must clean the RAM to prevent storage residue.

Time of check/time of use (TOC/TOU): This vulnerability is associated with multiprogramming and multiple processors, and it is a type of asynchronous attack. It can occur when a process passes pointers to parameters residing in its virtual memory to the operating system. At the same time, another process, with access to the memory area that contain the parameters, modifies the parameters between the time the operating system checks them and the time they are used.

Maintenance hooks: Maintenance hooks are part of the software code allowing easy maintenance; they are commonly called trapdoors or backdoors. These hooks form a risk on the software, so they should be removed prior the live implementation of the software (Hansche and others, 2004, P: 82-88).

2.3.1.2 Central Processing Unit (CPU) states

Processing Types

Computers must be designed in a way that they do not disclose information to an unauthorized recipient.

Single State: In single state systems, security administrators approve a processor and system to handle only one security level at a time.

Multi state: Multi state systems are certified to handle multiple security levels simultaneously by using specialized security mechanisms, such mechanisms are designed to prevent information from crossing between security levels.

Security Modes

Dedicated Mode: The user in this type of systems needs three requirements:

Each user must have: 1-Security clearance permitting him the access to all information processed by the system, 2-Access approval for all information processed by the system, and 3-Valid need to know for all information processed by the system.

System High Mode: The user in this type of systems also needs three requirements:

Each user must have: 1-Valid security clearance that permits access to all information processed by the system, 2-Access approval for all information processed by the system, and 3-Valid need to know for some information processed by the system.

Compartmented Mode: The user in this type of systems also needs three requirements:

Each user must have: 1-Valid security clearance that permits access to all information processed by the system, 2-Access approval for all information they will have access to on the system, and 3-Valid need to know for all information they will have access to on the system.

Multi level Mode: Following are the characteristics of this type of systems:

Some users do not have a valid security clearance for all information processed by the system.

Each user must have:

1-Access approval for all information they will have access to on the system.

2-Valid need to know for all information they will have access to on the system (Tittel and others, 2003, P: 374-377).

2.3.1.3 Memory Management Overview

There are many types of memory, such types are:

Cache memory: A small amount of very high speed RAM, which holds the instructions and data from primary memory. It moves these instructions to the higher speed cache in

anticipation of the CPU requiring these programs and data. Properly designed caches can significantly reduce the apparent main memory access time and thus, increase the speed of program execution.

Random Access Memory: Memory where locations can be directly addressed and the data that is stored can be altered. RAM is volatile due to the fact that the data is lost if power is removed from the system.

Programmable Logic Device (PLD): An integrated circuit with connections or internal logic gates that can be changed through a programming process. Examples of a PLD are a Read Only Memory (ROM), a Programmable Array Logic (PAL) device. This last technology is volatile because the power to the chip must be maintained for the chip to operate.

Read Only Memory (ROM): Non-volatile storage where locations can be directly addressed. In a basic ROM implementation, data cannot be altered dynamically. Non-volatile storage retains its information even when it loses power. Programs stored on these types of devices are referred to as firmware.

Real or primary memory: The memory directly addressable by the CPU and used for the storage of instructions and data associated with the program that is being executed. This memory is usually high-speed, RAM.

Secondary memory: This type of memory is a slower memory (such as magnetic disks) that provides non-volatile storage.

Sequential memory: Memory from which information must be obtained by sequentially searching from the beginning rather than directly accessing the location. A good example of a sequential memory access is reading information from a magnetic tape.

Virtual memory: This type of memory uses secondary memory in conjunction with primary memory to present a CPU with a larger, apparent address space of the real memory locations.

Memory protection

Means to prevent one program from accessing and modifying the memory space contents that belong to another program. Memory protection is implemented by the operating system or by hardware mechanisms (Krutz and Vines, 2001, P: 176-178).

2.3.1.4 Input/Output Devices

Monitors: It's a fact that when you turn monitor off, the data disappears from the screen and can't be recovered. However, a technology known as TEMPEST can compromise the security of data displayed on a monitor.

Printers: Printers also may represent a security risk. If printers are shared, users may forget to retrieve their sensitive printouts, leaving them vulnerable to other users.

Keyboards/Mice: Keyboards, mice, and similar input devices are not immune from security vulnerabilities either. All of these devices are vulnerable to TEMPEST monitoring. A simple device can be placed inside a keyboard to intercept all of the keystrokes that take place and transmit them to a remote receiver using a radio signal. This has the same effect as TEMPEST monitoring but can be done with much less-expensive gear.

Modems: If they are not configured properly, they can create serious security vulnerabilities that allow an outsider to bypass all of your perimeter protection mechanisms and directly access your network resources. It also allows insiders to funnel data outside of your organization (Tittel and others, 2003, P: 387-388).

2.3.1.5 Storage Devices

There are many types of storage devices, following are some of these types:

Floppy disk, Hard disk, Zip disk, CD-ROM, Rewritable CD, DVD, Flash memory, and Magnetic tapes. Some of these types can easily be transported and read on other computers, this can increase the risk of losing data if a security controls are not established (Hansche and others, 2004, P: 96-97).

2.3.2 Network Environment (Hansche and others, 2004, P: 97-100)

A network can be defined as a data communication system that permitting a number of devices to communicate with each other. Authors also added that, it allows its users to share common resources and to send and receive information.

2.3.2.1 Shared Environment

Client/server environment is the most common shared network systems, in this environment, the client is a PC or workstation, and the server provides users with some

shared services. The shared environments facing some threats; and following are some of these threats:

- Misconfigured file protection
- Database corruption
- Unsecured locations
- Multiple administrators
- Malicious code
- Lack of alarm notification
- Inconsistent user identification and authorization across shared environment

2.3.2.2 Types of security Environment

Dedicated security mode: it is the mode when the system is specifically dedicated for processing one type of information. A system operating in a dedicated mode when each user, peripherals, remote terminal, or remote hosts has all the following:

- A valid personal clearance for all information on the system.
- Formal access approval for all the stored and/or processed information
- A valid need-to-know for all information in the system.

System high-security mode: in this mode of operation, the system hardware/software is only trusted to provide need-to-know protection between users.

Multi-level security mode: in this mode of operation, two or more classification levels of information are allowed to be processed at the same time within the system when some users are not cleared for all levels of information.

Controlled mode: it is a type of the multi-level security mode in which a more limited trust is placed in the hardware/software base of the system, with resultant restrictions on the classification and clearance levels.

Compartmentalized security mode: in this type of operation, the system access is secured to the highest level of information, but it is not necessary for all users to be formally authorized access to all types of compartmented information (information requiring a special authorization) being processes and/or stored in the system.

2.3.3 Enterprise architecture (Murray, 2004, P: 2295- 2296)

Architecture is the part of design that deals with appearance, function, location, and materials.

2.3.3.1 Security Architecture

The security architecture describes the appearance of the security functions, and among other things it will describe the following:

Duties, roles, and responsibilities: The architecture will describe who is to do what and specifies upon who the management relies and for what..

How objects will be named: It will describe how objects such as users and information resources are named, identified or referred to in the enterprise.

What authentication will look like: It must describe how management will trust in these objects. It describes what evidence the user will provide to prove his/her identity.

Where it will be done: The architecture will describe where the authentication data are to be collected, where to be stored, and what process will reconcile the two.

What the object of control will be: The architecture must describe what it is that will be controlled. This could be a file, database, or a program.

Where access will be controlled: The architecture will describe where the control of access will be, for example it could be centralized in a single process overall the enterprise. In more modern systems access will be controlled in a large number of places, such places will be departments, applications.

Generation and distribution of warnings and alarms: Finally, the design must specify what events require corrective action, what process will detect them, who is responsible for the action, and how the warning will be communicated from the detecting process to the party responsible for the correction.

2.3.4 Security Models

The researcher found that there are many security models, but in the following section two of them will be described; such models are Bell-LaPadula and Biba Security Model.

2.3.4.1 Bell-LaPadula Security Model

The Bell-LaPadula model was developed out of the U.S. Department of Defense (DoD) multilevel security policy. That policy includes four levels of security classification; such levels are top secret, secret, confidential, and unclassified. The DoD policy states that a subject with any level of clearance can access resources at or below their clearance level.

In Bell-LaPadula model, and as it shown in figure (2.4), secure states are constrained by the following two rules:

Simple Security Property*:* The SS Property states that a subject at a specific classification level cannot read data with a higher classification level. This is often shortened to "no read up."

**** Security Property*** The (star) * Property states that a subject at a specific classification level cannot write data to a lower classification level. This is often shortened to "no write down."

The Bell-LaPadula efficiently manages confidentiality, but it fails to manage the following important issues:

- It does not deal with integrity or availability.
- It does not deal with access control management.
- It does not provide a way to assign or change an object's or subject's classification level.
- It does not address file sharing (Tittel and others, 2003, P: 18-20).

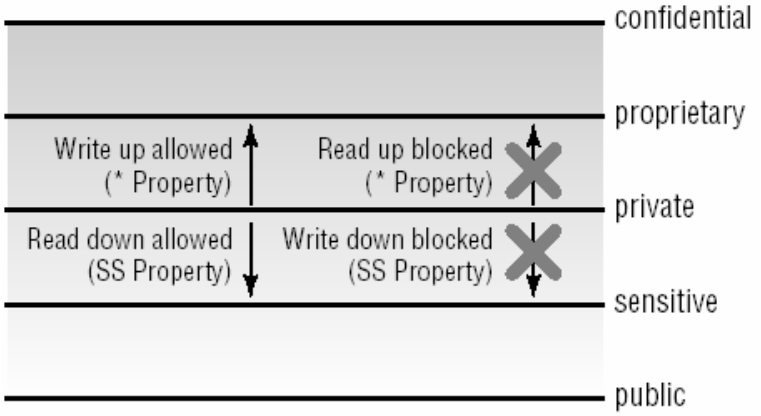


Figure (2. 4): The Bell-LaPadula model
Source: (Tittel and others, 2003, P: 19)

2.3.4.2 Biba Security Model

Biba has two integrity axioms as it is shown in (Figure 2.5):

Simple Integrity Axiom: The SI Axiom states that a subject at a specific classification level cannot read data with a lower classification level. This is often shortened to “no read down.”

*** Integrity Axiom:** The (star) * Axiom states that a subject at a specific classification level cannot write data to a higher classification level. This is often shortened to “no write up.”

The critiques of the Biba model mention a few drawbacks:

- It only deals with integrity, not confidentiality or availability.
- It focuses on protecting objects from external threats; it assumes that internal threats are handled programmatically.
- It does not deal with access control management.
- It does not provide a way to assign or change an object’s or subject’s classification level.

Another important security models are Clark-Wilson, Information flow model, Noninterference model, Take-Grant model, and Access control matrix (Tittel and others, 2003, P: 18-20).

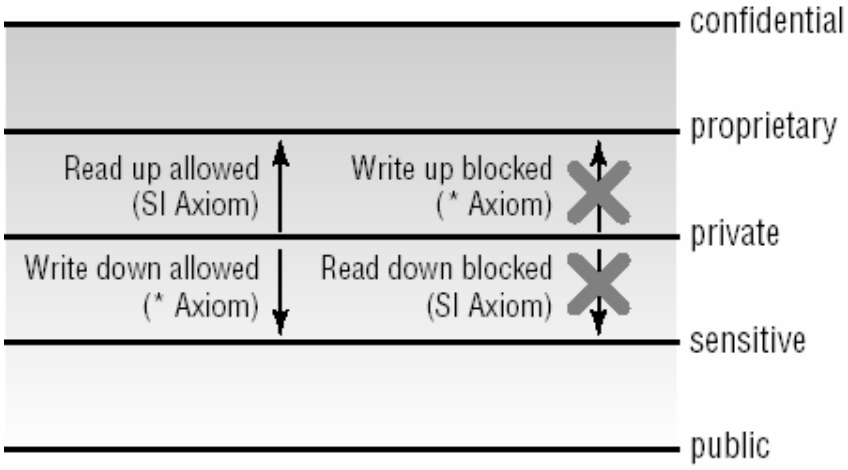


Figure (2. 5): Biba model
Source: (Tittel and others, 2003, P: 20)

2.3.5 Protection Mechanisms

As a result of findings of Seventh Annual 2002 Computer Crime and Security Survey and others, the protection mechanisms are becoming required more than before with keeping in mind that no system can be totally secured.

Layering: Layering refers to the organization of separate functions that interact in a hierarchal sequence. A good example for layering is the OSI model that contained of seven layers stacked upon each other and there is an interaction among those layers.

Abstraction: System administrators and programmers should be familiar with abstraction. Object-oriented programming uses abstraction. Abstraction is about removing the characteristics from an entity in order to easily represent its essential properties. For example, it is easier for a system administrator to grant rights to a group than to grant it to members.

Data Hiding: Think of Windows 2000 Professional Operating System as an example. The printer icon contains information related to a specific printer. The information on this specific object is predefined. The object only needs to know certain information to complete its task. But other information like IRQ, port, and protocol should be used to execute this task? What is the memory space address? Does the user have sufficient rights to print? This means that any information not needed to carry out the print task is hidden from the printer object.

Principle of least privilege: Programs and users should only be given access to the resources that are necessary for completing their tasks. Access to privileged resources should be removed when a process has been done (Henderson, 2004, P: 2478-2479).

2.4 Access Control Systems and Methodology

Three topics will be discussed in this section, these topics are Access Control Policy, Threats, and Security Technology and Tools.

2.4.1 Access Control Policy

Organizations need to control the access of the users to the system components and resources in order to protect its information; from here the identification and authentication came. After the user accesses the system, he needs permissions in order to do his/her duties

and tasks in that system, so a written access control policy will be very useful in showing who allowed doing what, such thing called the authorization. The access control policy is based on Separation of Duties and Least Privilege practice (Hansche and others, 2004).

2.4.1.1 Separation of Duties

Separation of duties is an administrative control, which can be implemented by defining the elements of the process or the work function, and then dividing those elements among the different employees.

This prevents one employee from obtaining control of an entire process; such employee needs to conduct an agreement with others in order to manipulate the process for personal gain (Hansche and others, 2004).

2.4.1.2 Least Privilege

The Least Privilege term is known in some organizations as “need-to-know”, which permit the user to only access the resources that needed for him to implement his/her tasks and duties, no more and no less. This to ensure that no users can access resources he/she should not do. In order for an organization to have Least Privilege policy, some groups or levels should be identified according to the types of tasks or work processes, and the users should be assigned to these groups (Hansche and others, 2004).

“Least privilege requires that each subject be granted the most restricted set of privileges needed for the performance of their task” (Krutz and Vines, 2001, P:214).

2.4.2 Threats

Information systems threats will be discussed in this topic, such threats are Transmission threats, Malicious code threats, and Password threats.

“A threat is simply any event that, if realized, can cause damage to a system, and create a loss of confidentiality, availability, or integrity. Threats can be malicious — such as the intentional modification of sensitive information — or they can be accidental — such as an error in a transaction calculation or the accidental deletion of a file.” (Krutz and Vines, 2001, P: 223).

As shown in Figure (2.6) which is based on (2007 CCSS); 64% of respondents said that they experience a security incident in the pas 12 months.

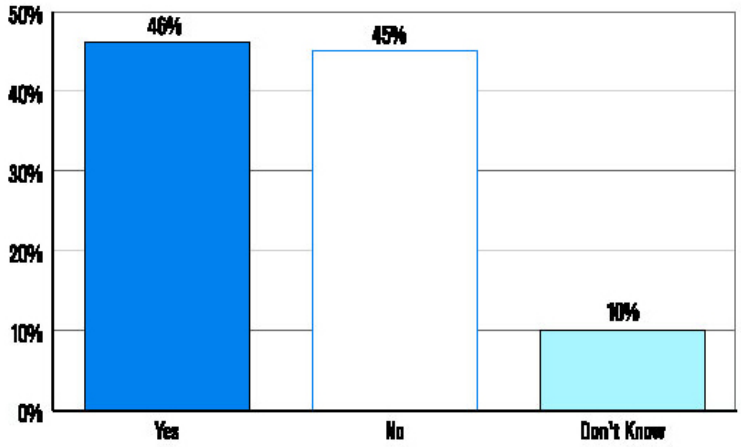


Figure (2. 6): Organizations Experiencing Security Incidents
Source: (2007 CCSS) http://www.gocsi.com, (Jan 2008)

Figure (2.7) shows the number of incidents that the respondents experienced in the past 12 months of the survey conduction.

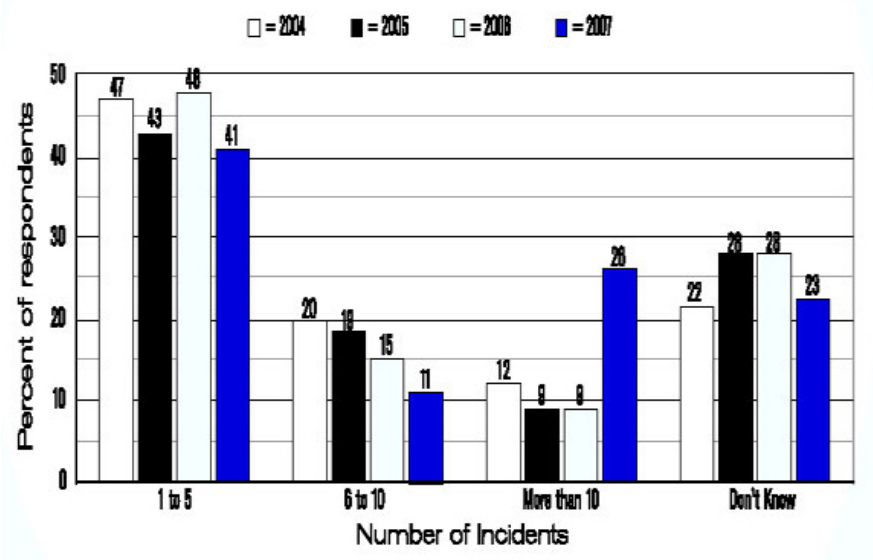


Figure (2. 7): Number of Security Incidents
Source: (2007 CCSS) http://www.gocsi.com, (Jan 2008)

The threats that could affect the information security are increasing in a daily basis because of the increasing and extension of the businesses that depend on the information systems and computer networks. So it is not easy to count all the threats of information systems, and here are some types of information systems threats.

2.4.2.1 Transmission Threats

-Denial-of-Service (DOS): They are attacks which prevent the system from processing or responding to legal requests for resources and objects. The most common form of denial of service attacks is transmitting so many data packets to a server which make it very busy and cannot process them all (Tittel and others, 2003).

Denial of Service is the common name of the attacks on resource availability. It occurs when invalid data is sent in such a way that confuses the server software and causes it to crash.

The denial of service threat not intending to stealth or damage information, its objective is to make that resource to stop functioning and make it not accessible by the authorized users. One example of such threat is to flood a mailbox with a unwanted email messages to make that email box full, which means he/she cannot receive the normal business messages (Hansche and others, 2004).

Distributed Denial-of-Service (DDoS): it occurs when the attacker compromises several systems and uses them as launching platforms against one or more victims. The compromised systems used in the attack are often called slaves or zombies..

The compromised systems (called zombies) could be in hundreds or thousands, which means an army of computers or systems attacking the victim by sending it a lot of data packets, the victim computer in this case cannot process or handle that value of data, then it will not be able to serve the authorized users (Tittel and others, 2003).

Ping of Death: The ping program is used in the normal situation to check if a remote host on the network is operating. The ping sends a packet (a tiny piece of data) to the remote

host and waiting that host to reply; if the remote host sending a reply packet that means it is operating and there is a connection between the sender and the receiver machines.
The ping of death attack is initiated by sending a 65,535 bytes long packet which is not valid, but this would be possible because packets are broken into fragments for transmission, in this case, the receiver system will not process a packet until all packets received and reassembled into one packet. The long packet will cause an overflow in the system's internal buffers which make the system to crash (Hansche and others, 2004).
The ping of death attack is a type of attack on a computer that involves sending a malformed or malicious ping to a computer. A ping is normally 64 bytes in size (or 84 bytes when IP header is considered); many computer systems cannot handle a ping larger than the maximum IP packet size, which is 65,535 bytes.[1]

2.4.2.2 Malicious Code Threats

It is a code that can get access to a system and violates security policy. It includes various types of rogue code, such as viruses, worms, Trojan horses, and logic or time bombs" (Hansche and others, 2004, P: 161).

Viruses: "A computer virus is a malicious program designed to damage network equipment, including stand-alone computers. A virus has two parts: the application that activates and spreads the virus, and the "payload," which is what the virus does to the operating system or file." (Stanger and others, 2002, P: 139).
A virus may also damage your data files, operating systems, and spreads to the computers on the network. It can infect your computer through the CD-ROM, Floppy disk or email (Pastor and Dulaney, 2004).

Worms: "Worms are programs that reproduce by copying themselves through computers on networks" (Hansche and others, 2004, P: 162).

Trojan horse: "A Trojan horse is a code fragment that hides inside a program and performs a disguised function" (Hansche and others, 2004, P: 162).

[1] http://en.wikipedia.org/wiki/Ping_of_death (23 Jun 2007)

2.4.2.3 Password Threats

Passwords can be attacked when: The user creates a weak password. Sniffers can stealth the password while it's transmission through the network. Recoding the keyboard clicks. By installing a Trojan horse in the victim's computer (Hansche and others, 2004).

Appendix (3) shows the types of attacks and misuses that detected in the year of 2007, the information is extracted from (2007 CCSS).
Appendix (4) also shows the dollar amount losses by type of attack.

2.4.3 Security Technology and Tools

We will discuss Access to the systems and Access to the data under the security technology and tools topic.

2.4.3.1 Access to the system

Identification: "Identification is the act of a user professing an identity to a system, usually in the form of a log-on ID to the system. Identification establishes user accountability for the actions on the system." (Krutz and Vines, 2001, P: 39)

Authentication: Authentication is to verify the validity of the user's identity which implemented through a user password at log-on time. Authentication is based on the following three factor types: some thing you know, something you have, and something you are (Krutz and Vines, 2001).

Password: Something You Know

"Passwords are used to verify that the user of an ID is the owner of the ID. The ID-password combination is unique to each user and therefore provides a means of holding users accountable for their activity on the system." (Tipton, 2004, P: 119).

Smart Cards : Something You Have

"Smart cards are usually about the size of a credit card and contain a chip with logic functions and information that can be read at a remote terminal to identify a specific user's privileges. Smart cards now carry prerecorded, usually encrypted access control information that is compared with data that the user provides (e.g, a personal ID number or biometric data) to verify authorization to access the computer or network." (Tipton, 2004, P: 119).

Fingerprint: Something You Are

Fingerprint is considered the most popular biometric characteristic for identification and authentication. Our finger contains a large number of ridges and furrows on the surface of the fingertips. In the fingerprint scanning systems the user puts his/her finger on an optical or silicon surface for two to three seconds. And there are two types of the scanning systems, first is the optical scan which scans a visual image of the fingerprint, and the second is to electronically capture the image of the finger by generating electrical field. Other types of biometric characteristics are Hand geometry, Voice pattern, Iris pattern, and Signature dynamics (Fried, 2004, P: 59-61).

2.4.3.2 Access to Data

Rule-Based Access Control: In this type of controls, the system owner creates a list of rules and determines the privileges into these rules, then specifying the rules to the users; such privileges could be read, written, executed.

Role-Based Access Control: In role based access control, the access to the data is based on the tasks and functions that the user is allowed to perform. Any trusted user to perform such role granted the authorization into that role in order to complete his tasks and functions in the organization.

Content-Based Access Control: In content based access control, the access to the data is based on the content of the object. For example, software program that preventing the access to some websites from the organization's computers (Hansche and others, 2004).

2.5 Applications and Systems Development

Three main topics will be discussed in this section, first is the Application Environment, second is the Databases and Data Warehousing, and third is Systems Development Life Cycle Methods.

2.5.1 Application Environment

In this section, Local Environments and Distributed Environment will be discussed.

2.5.1.1 Local Environment

In local or non distributed computing environment, individual computer systems store and execute programs to perform functions for the local user. Such functions could interact with networked applications that provide access to remote resources, such as web servers, mail servers, and file servers. One key characteristic of local systems is that the application code executed locally in the local computer, even if it is using some remoter resources such as files in a shared network resource (Tittel and others, 2003).

There are many threats that could face the local computing environment, and here are some of them:

Viruses: "A virus is a fragment of code that attaches itself to other executable computer instructions, including software application code, the code used to boot the computer, and macro instructions placed in documents. A key component of a virus is the ability to replicate and reproduce itself on the system; generally, a virus requires some type of action by the user or a process to activate." (Hansche and others, 2004, p: 232).

As shown in Appendix (4), the losses amount that viruses (Worms/Spyware) caused to the organizations that respond to (2007 CCSS) was $8,391,800.

Trojan horses: A Trojan horse is a malicious code object that you think of as a useful program, when you execute; it performs the advertised functions; however, electronic Trojan horses also carry an unknown payload. While you are using that program, the Trojan horse also performs some sort of malicious action—such as opening a security holes

in the system for hackers to do some actions in your computer without your knowledge (Tittel and others, 2003).

Logic bombs: Logic bombs are programs that run when a certain event occurs. A bomb may send a message informs the attacker that the user is ready for an attack. We can notice that this bomb does not actually begin the attack, but tells the attacker that the victim has met the needed state for an attack to begin. Logic bombs may also be set to go off on a certain date or when a specified set of circumstances occurs (Pastor and Dulaney, 2004).

Worms: "Worms are an interesting type of malicious code that greatly resemble viruses, with one major distinction. Like viruses, worms spread from system to system bearing some type of malicious payload. However, whereas viruses must be shared to propagate, worms are self-replicating. They remain resident in memory and exploit one or more networking vulnerabilities to spread from system to system under their own power. Obviously, this allows for much greater propagation and can result in a denial of service attack against entire networks." (Tittel and others, 2003, P: 210).

2.5.1.2 Distributed Environment

Distributed computing allows a user to exploit the computing power of one or more remote systems. A common example of this is the client/server interaction that occurred when Internet browser tried to access a web page; in this case, the web server that hosts the website is responding to the client's request and sending it back the required content (Tittel and others, 2003).

Agents: Agents (also known as bots) are intelligent code objects that perform actions on behalf of a user. Agents typically take initial instructions from the user and then carry on their activity in an unattended manner for a predetermined period of time, until certain conditions are met, or for an indefinite period (Tittel and others, 2003).

Applets: "This a Java program that can be embedded in a Web page. The difference between a standard Java application and a Java applet is that an applet can't access system

resources on the local computer. System files and serial devices (modems, printers, scanners, etc.) cannot be called or used by the applet. This is for security reasons -- nobody wants their system wiped out by a malicious applet on some wacko's Web site." (http://www.iwebtool.com/what_is_applet.html, Oct/2007)

2.5.2 Databases and Data Warehousing

All businesses today are relying on database systems, so; information security professionals need to ensure that the best security controls are applied to protect these systems against unauthorized access or destruction of data (Tittel and others, 2003).

"A data warehouse is a repository of information from heterogeneous databases that is available to users for making queries. Data in the data warehouse is normalized — redundant data is removed. Thus, data in the warehouse is extracted and refined, and it is available for access and analysis." (Krutz and Vines, 2001, P: 245).

2.5.2.1 Database Management System (DBMS) Architecture

A Database Management System (DBMS) is a collection of applications that manage large and structured sets of persistent data. It stores, maintains, and provides access to data using query capabilities (Hansche and others, 2004)

Multilevel Security: "Multilevel security databases contain information at a number of different classification levels. They must verify the labels assigned to users and, in response to user requests, provide only information that's appropriate." (Tittel and others, 2003, P: 216).

Database Vulnerabilities and Threats

The threats to a DBMS include:

Aggregation: Aggregation is the ability to combine non sensitive data from different sources to make sensitive information (Hansche and others, 2004).

Tittel and others (2003) state that: Standard Query Language SQL provides a number of aggregation functions that can be used to collect some information from the database, and

that information could be considered as a sensitive data. The aggregation functions include: Count, Min, Max, Sum, and Avg.

Bypass attacks: "Users attempt to bypass controls at the front end of the database application to access information. If the query engine does not have any security controls, the engine may have complete access to the information; thus, users may try to bypass the query engine and directly access and manipulate the data" (Hansche and others, 2004, P: 255).

Denial-of-service: "This refers to any type of attack or action that could prevent authorized users from gaining access to the information. Often, this can happen through a poorly designed application or query that locks up the table and requires intensive processing" (Hansche and others, 2004, P: 255).

2.5.3 Systems Development Life Cycle Methods

There are many models used in the systems development life cycle, and here are two of these models:

2.5.3.1 The Waterfall Model

It is the oldest known model for developing software systems, and it is consisting of phases and each phase contains a list of activities that must be done and documented before the next phase starts. The waterfall mode has two disadvantages, one: it is does not scale well for large and complex projects. Second: because every phase must be done before the next one start, this could inhibit the team from working around concurrent phases or activities (Hansche and others, 2004). The waterfall model is shown in Figure (2.8).

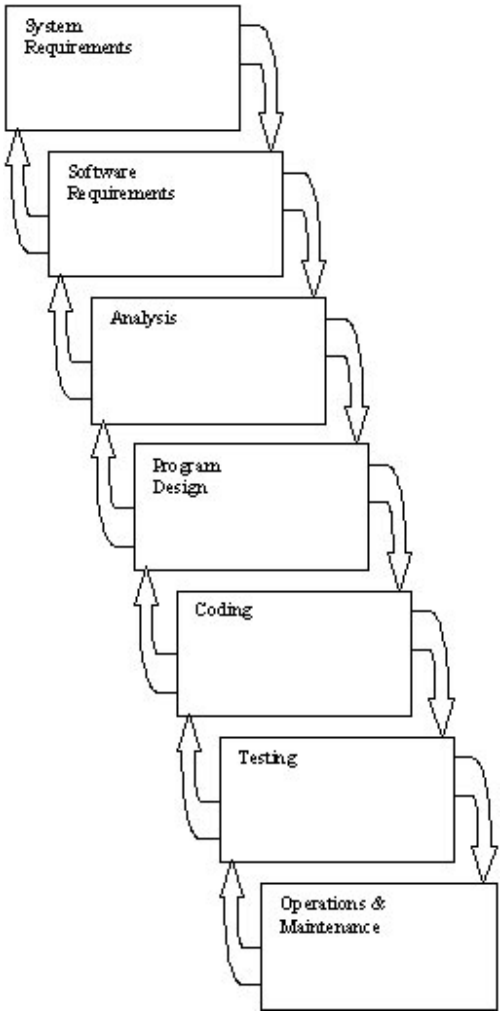


Figure (2. 8): The waterfall Model
Source: (Krutz and Vines, 2001, P:235)

2.5.3.2 The Spiral Model

The Spiral Model was proposed in 1988 as an alternative life cycle model that allows for multiple iterations of a waterfall-style process. And as shown in Figure (2.9), each "loop" of the spiral results in the development of a new system prototype (represented by Prototype 1, Prototype 2, and Prototype 3 in the illustration). Theoretically, system developers would apply the entire waterfall process to the development of each prototype (Tittel and others, 2003).

One of the spiral model features is that it added a risk assessment review in each phase (Hansche and others, 2004).

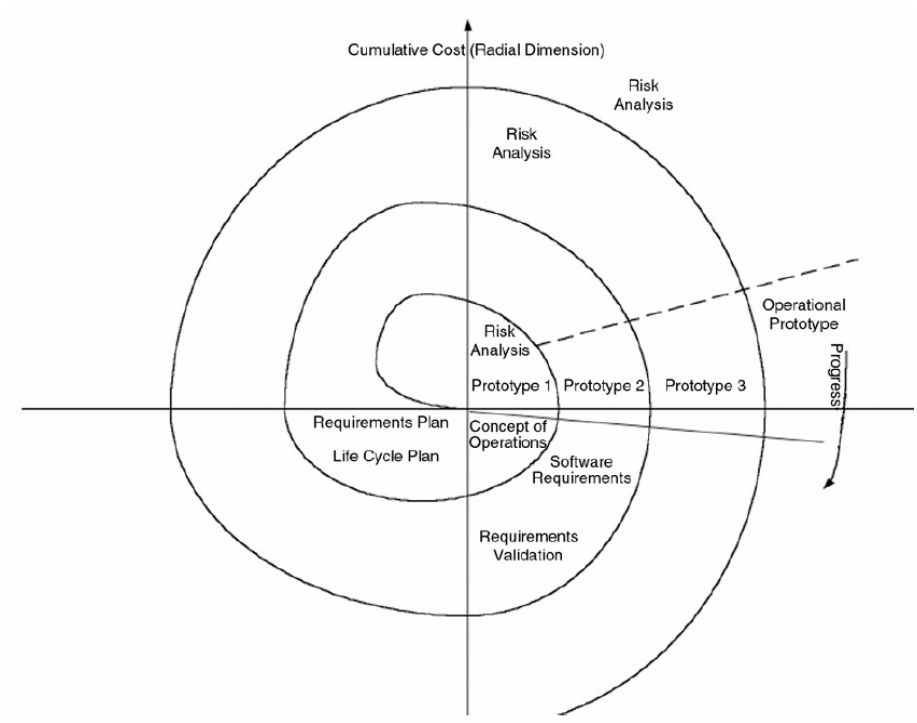


Figure (2. 9): The Spiral Model
Source: (Krutz and Vines, 2001, P: 237)

2.5.3.3 Software Development Phases

Hansche and others (2004, P: 265 – 273) argue that there are typical phases need to be included in the software development process regardless of the used model, and here are these phases and security activities that should be implemented in parallel with each phase activities:

- **Project initiation and planning**

  The security activities through this phase should be:

  - Identify Security Needs: Classification and criticality of information and/or applications, basic security objectives, and security controls workloads.
  - Initial Risk Analysis: Threats, vulnerabilities and risks are identified.
  - Technical, operational, and economical feasibility of security alternatives are analyzed. And security-related costs/benefits are estimated.

- Identify Security Framework: Essential security issues and risks, and determination of service level agreement.

- **Functional requirements definition**
  - Security areas in project plan: Configuration and access controls, and Audit trails.
  - Define Security requirements: Risk analysis and contingency plan.
  - Preliminary security test plan: Test methods and resources.
  - Include security requirements in request for proposals and contracts.
  - Functional baseline has security requirements
- **System design specifications**
  - Define security specifications: Systems/subsystem/interface, and program/database/hardware and firmware/network.
  - Update security test plan: Develop test procedure, and test security under abnormal and illegal circumstances.
  - Include security are in formal baseline documentation and quality assurances.
- **Build/develop and document**
  - Write or procure and install security related code.
  - Perform unit test and evaluate security related code.
  - Ensure approved security components in formal baseline are included.
- **Acceptance**
  - Test security components
  - Test security in integrated system.
  - Install security code with necessary modifications.
  - Document security controls.
  - Conduct acceptance test.
  - Accept/verify project security.
- **Transition to production**
  - Verifying that the data conversion and data entry are controlled and only those who need to have access during this process are allowed on the systems.
  - An acceptable level of risk is determined and security accreditation is obtained.

- Applying some controls to validate the accuracy of information after it is entered into the system.

- **Operations and maintenance support**
  - Testing backup and recovery procedures.
  - Ensuring proper controls for data and report handling.
- Revisions and system replacement
  - Reviewing security planning and procedures to avoid future problems.
  - Conducting application audits and documenting security incidents.
  - Documenting system failures.

2.6 Operations Security

In this section, three topics will be discussed as main parts of the operations security, such topics are Types of Security Controls, Operations Security Controls, Auditing and Audit Trails, and Monitoring Techniques.

2.6.1 Types of Security Controls

Directive Controls: Usually called administrative controls; their purpose is to advice the employees on how their behavior should be when they interact with organization's information systems. These directives always presented as policies or related documents.

Preventive Controls: Preventive controls are mechanisms to prevent undesirable actions to be occurred. Some examples of these controls are guards, mantraps, backups, UPS, separation of duties, and user registration.

Detective Controls: They are about using practices, processes, and tools that detect and react to security violations. Some examples of these controls are audit trails, intrusion detection, logs, and violation reports.

Corrective Controls: These controls contain a physical, administrative, and technical measures designed to react to any detection of an incident in order to reduce or eliminate its occurrence again.

Recovery Controls: Once a violation has occurred, recovery controls are necessary to restore the system or operation to its normal operating state. The recovery control could be restoring a lost or corrupted file from the backup (Hansche and others, 2004, P: 341–342).

2.6.2 Operations Security Controls

In this topic, six issues will be discussed, such issues are Resource protection, Hardware controls, Software controls, Privileged entity controls, Media resource protection, and Physical access controls.

2.6.2.1 Resource protection

Resource protection is about protecting an organization's computing resources and assets from loss or compromise, such resources are defined as any hardware, software, or data that used and owned by the organization. Resource protection is about reducing the possibility of damage which can result from unauthorized disclosure or alteration of data. And here are some resources that require protection according to the authors:

Hardware resources: Communication devices, Storage media, Processing systems, Standalone computers, and Printers and fax machines,

Software Resources: Program libraries and source code, Operating system, and systems utilities.

Data Resources: Backup data, User data files, Password files, Operating Data Directories, and System logs and audit trails (Krutz, and Vines, 2001, P: 216-219).

2.6.2.2 Hardware controls

Hardware Maintenance: System maintenance could be performed by staff, vendor, or service provider. And it could be done inside or outside the organization. A background check for the service personnel may be necessary.

Maintenance Accounts: Many computer systems present maintenance accounts, which are supervisor level accounts and created at the factory with widely known passwords. Disabling such accounts is critical until they needed.

Diagnostic Port Control: Many systems have diagnostic ports for troubleshooting purpose; these ports should only be used by authorized persons, and should not enable neither internal nor external unauthorized access.

Hardware physical control: The data processing areas that contain the hardware should be physically protected by alarms and locks (Krutz, and Vines, 2001).

2.6.2.3 Software controls

Anti-Virus Management: The user's ability to load or execute programs makes the system more vulnerable to viruses, unexpected software behavior and destroyed security controls.

Software Testing: A formal software testing process should by applied to make sure that the software is compatible with other applications

Software Utilities: The use of powerful systems utilities must be controlled by a security policy, because it can compromise the integrity of operations systems and logical access controls.

Safe Software Storage: Both of logical and physical access controls should be implemented in the place to ensure that the software and copies of backups have not been modified without proper authorization.

Backup Controls: It is very important to routinely test the restore accuracy of a backup system. A backup should also be stored securely to protect from theft, damage, or environmental problems (Krutz, and Vines, 2001, P: 216-218).

2.6.2.4 Privileged entity controls

Privileged entity access is defined as special access to computing resources given to operators and system administrators. It is also known as privileged operations functions. Special access to system commands, Access to special parameters, and Access to the system control program are some examples of privileged entity operator functions (Krutz, and Vines, 2001).

2.6.2.5 Media resource protection

Media Security Controls: Are implemented to prevent any threat to C.I.A. by the exposure of sensitive data, they should be designed to prevent the loss of sensitive information when the media is stored outside the system, and here are some elements of media security controls:

Logging: Logging the use of data media provides accountability and assists in physical inventory control.

Access Control: Physical access control to the media is used to prevent unauthorized personnel from accessing the media.

Proper Disposal: Proper disposal of the media after use is required to prevent data recovery.

Media viability controls: Many physical controls should be used to protect the viability of the data storage media. The goal is to protect the media from damage during handling and transportation, or during short-term or long-term storage. Proper marking and labeling of the media is required in the event of a system recovery process:

Marking: All data storage media should be accurately marked or labeled. The labels can be used to identify media with special handling instructions, or to log serial numbers or bar codes for retrieval during a system recovery.

Handling: Some issues with the handling of media include cleanliness of the media and the protection from physical damage during transportation to the archive sites.

Storage: Storage of the media is very important for both security and environmental reasons. A proper heat- and humidity-free, clean storage environment should be provided for the media. Data media is sensitive to temperature, liquids, magnetism, smoke, and dust (Krutz, and Vines, 2001).

2.6.2.6 Physical access controls

Following are examples of some of the elements of the operations resources that need physical access control.

Hardware: Control of communications and the computing equipment, Control of the storage media, and Control of the printed logs and reports.

Software: Control of the backup files, Control of the system logs, Control of the production applications, and Control of the sensitive/critical data.

Personnel: Some personnel will require special physical access to perform their job functions. The following are examples of this type of personnel:

-IT department personnel

-Cleaning staff

-Heating Ventilation and Air Conditioning (HVAC) maintenance personnel

-Third-party service contract personnel

-Consultants, contractors, and temporary staff (Krutz, and Vines, 2001).

2.6.3 Auditing and Audit Trails

Operations security Auditing and Audit trails will be discussed in this topic as a follow up and monitoring issues.

2.6.3.1 Auditing

Auditing is a methodical examination or review of an environment to ensure compliance with regulations and to detect abnormalities, unauthorized occurrences, or outright crimes. Secure IT environments rely heavily on auditing.

Auditing covers a wide variety of different activities, logging, monitoring, examining alerts, analysis, and even intrusion detection.

Logging: Logging is the activity of recording information about events or occurrences to a log file or database.

Monitoring: Monitoring is the activity of manually or programmatically reviewing logged information looking for something specific.

Alarm triggers: Alarm triggers are notifications sent to administrators when a specific event occurs.

Log analysis: Log analysis is a more detailed and systematic form of monitoring in which the logged information is analyzed in detail for trends and patterns as well as abnormal, unauthorized, illegal, and policy-violating activities.

Intrusion detection: Intrusion detection is a specific form of monitoring both recorded information and real-time events to detect unwanted system access (Tittel and others, 2003, P: 464-465).

2.6.3.2 Audit trails

Audit trails are the records contained information about events and occurrences into a database or log file. Audit trails are used to reconstruct an event, to extract information about an incident, to prove or disprove responsibility, and much more. They allow events to be examined or traced in forward or reverse order. This flexibility is useful when tracking down problems, coding errors, performance issues, attacks, intrusions, security breaches,

and other security policy violations. Using audit trails is a passive form of detective security control (Tittel and others, 2003, P: 466-467).

2.6.4 Monitoring Techniques

Intrusion detection, Penetration testing, and Violation analysis issues will be discussed in this topic.

2.6.4.1 Intrusion detection

Intrusion Detection (ID) is a useful tool that can assist in the detective analysis of intrusion attempts, (Krutz and Vines, 2001) argue. Authors also added that ID can be used for the identification of intruders. By analyzing the activities a security practitioner can find evidence of events of system abuses.

2.6.4.2 Penetration testing

Penetration testing is the process of testing a network's defenses by trying to access the system from the outside using the same techniques a cracker would use. This testing gives a security practitioner a better snapshot of the organization's security position.

Here are some techniques used to perform a penetration test:

Scanning and Probing: A port scanner can tell information about a network's infrastructure and enable the intruder to access unsecured ports.

Demon Dialing: Demon dialers test all phone lines to try to locate modems that are attached to the network, which provide information that can then be used to attempt external unauthorized access.

Sniffing: A protocol analyzer can be used to capture data packets that are then decoded to give information such as passwords (Krutz and Vines, 2001, P: 220-221).

2.6.4.3 Violation analysis

Violation tracking, processing, and analysis is one of the most used techniques to track irregularity in user activity. To make violation tracking effective, clipping levels must be established. A clipping level is the routine level of user errors. It is used to enable a system

to ignore normal user errors. And when it is exceeded, a violation record is then produced (Krutz and Vines, 2001).

The most security technologies used in U.S. organizations are shown in the Appendix (5), the information was extracted from (2007 CCSS).

2.7 Cryptography

In this section two main topics will be discussed, the first is Basic concepts of cryptography and the other is Public Key Infrastructure PKI

(Gove, 2004, P: 2078) has identified the cryptography as "Cryptography is the study of the means to do encryption. Thus cryptographers design encryption systems. Cryptanalysis is the process of figuring out the message without knowledge of the cryptovariable (key), or more generally, figuring out which key was used to encrypt a whole series of messages."

Another identification is for (Purser, 2004, P: 60-61) who identified the Cryptography as the art of hiding information by transforming it in a way that a certain group of people can retrieve it in its original form and everyone else cannot. This is achieved by using some kind of key to effect the transformation. The parties that are allowed to retrieve the original information are provided with a key to undo the transformation.

2.7.1 Basic concepts of cryptography

The basic concepts of cryptography will be discussed in this topic, such concepts are Methods and Keys of cryptography, Symmetric Key Cryptography, and Asymmetric Key Cryptography.

2.7.1.1 Fundamentals: Method and Key

When people need to protect some valuable assets, they use locks which may be identically designed. But what makes each lock individually secure?

It is the combination, which is the key. The lock itself is the method or the algorithm. Together, the method and the key determine overall security strength of any cryptography technique (Hansche and others, 2004).

2.7.1.2 Symmetric Key Cryptography

It is the more traditional form of cryptography, in which, a message is encrypted and decrypted by using a single key. The secret key is shared between people who keeping it to themselves. Data encrypted with a secret key can be decrypted only with the same secret key.

Symmetric key is fast and suitable for encrypting a large amount of data. Symmetric key cryptography also called “private key cryptography”.

The primary problem of symmetric key cryptography is with key management, which is related to how the sender and receiver can agree upon and exchange the secret key without any possibility that an attacker can get access to it.

Another problem is the scalability, which related to the huge number of needed keys because of the increase of the communicated parties that use such type of cryptography.

Advantages: Speed, Strength, and Availability of algorithm.

Disadvantages: Key management and implementation, Key distribution, and Limited security (Hansche and others, 2004, P: 399-401).

2.7.1.3 Asymmetric Key Cryptography

This technique came to solve the key management problem in the symmetric key cryptography. It uses the “public key” concept, and called public key cryptography.

In asymmetric key cryptography, each user has a public key and a private key. The public key is made public, while the private key remains secret. No need for the sender and receiver to share or transmit the private key information.

The idea behind asymmetric key cryptography is: if you encrypt the data by using private key, then you can decrypt by using the public key and vice versa. This can work because the two keys are linked to each other mathematically.

It is theoretically possible for an attacker to attack asymmetric key system by deriving the private key from knowledge of the public key.

Asymmetric key cryptography uses the concept of “hard math”, so it will be very difficult to attack it because it involved a very sophisticated mathematics.

To encrypt a message using asymmetric key cryptography, the sender would use the receiver’s public key to encrypt the message and send it. The receiver would then use his

private key to decrypt the message. No one listening in on the communications line can decrypt the message because the receiver is the only one who has the corresponding private key that can decrypt that message.

Advantages: Key management, Scalability, and Provides a full range of information security services.

Disadvantages: Computationally intensive and slow (Hansche and others, 2004, P: 401-403).

2.7.2 Public Key Infrastructure PKI

(Krutz and Vines, 2001, P: 156) argue that the integration of digital signatures and certificates, and the other services that required for E-commerce is called the Public Key Infrastructure (PKI). Such services provide integrity, access control, confidentiality, authentication, and non-repudiation for electronic transactions.

The modern security architectures are aiming to protect and distribute information that is needed in a widely distributed environment (Khun and others, 2001) argue. The authors also added that the emerging approach to address these security needs makes use of the scalable and distributed characteristics of PKI.

PKI allows you to conduct business electronically with the confidence that:

- The person or process sending the transaction is actually the originator.
- The person or process receiving the transaction is the intended recipient.
- Data integrity has not been compromised.

2.7.2.1 Certificate Authorities

The Certification Authority (CA) is a collection of computer hardware, software, and the people who operate it. The CA is known by two attributes: its name and its public key. The CA performs four basic PKI functions: issues certificates; maintains certificate status information and issues Certificate Revocation Lists (CRLs); publishes its current certificates and CRLs; and maintains archives of status information about the expired certificates that it issued. To fulfill these requirements, the CA may delegate certain functions to the other components of the infrastructure.

When a CA issues a certificate, it is declaring that the subject (the entity named in the certificate) has the private key that corresponds to the public key contained in the certificate. The CA may include additional information in the certificate which is corresponds to the subject. This additional information might be contact information, or policy information (Khun and others, 2001).

2.7.2.2 Registration Authorities

Registration Authorities (RA) are designed to verify certificate contents for the CA. Certificate contents may reflect information presented by the entity requesting the certificate. They may also reflect information provided by a third party such as the credit card limit which obtained from credit bureaus. The certificate may reflect information from company's departments or management. The RA aggregates these inputs and provides this information to the CA.

Unlike a CA, an RA will often be operated by a single person. Each CA will maintain a list of accredited RAs. An RA is known to the CA by a name and a public key. By verifying the RA's signature on a message, the CA can be sure an accredited RA provided the information, and it can be trusted. As a result, it is important that the RA provide adequate protection for its own private key (Khun and others, 2001).

2.7.2.3 PKI Repository

A repository is a database of active digital certificates for a CA system. The main business of the repository is to provide data that allows users to confirm the status of digital certificates for individuals and businesses that receive digitally signed messages.

PKI applications are heavily dependent on an underlying directory service for the distribution of certificates and certificate status information. The directory provides a means of storing and distributing certificates, and managing updates to certificates. Directory servers need to be interoperable; without such interoperability, a relying party will not be able to retrieve the needed certificates and CRLs from remote sites for signature verifications (Khun and others, 2001).

2.7.2.4 Archives

An archive is a database of information, and its used to store and protect sufficient information to determine if a digital signature on an old document should be trusted.

An archive takes the responsibility for long term storage of archival information on behalf of the CA. An archive makes sure that the information was good when it was received, and has not been modified while in the archive. The CA should provide sufficient information to determine if a certificate was actually issued by the CA as specified in the certificate and valid at that time (Khun and others, 2001).

2.7.2.5 PKI users

PKI users are organizations or individuals that use the PKI, but do not issue certificates. They rely on the other components of the PKI to obtain certificates, and to verify the certificates of other entities that they do business with (Khun and others, 2001).

2.8 Physical Security

Physical security can be defined as the countermeasures taken to make sure that something or some one is safe against theft, espionage, sabotage, or harm.

Physical security is the oldest form of protection. For ages, people have been working on protecting themselves from harm and their valuable assets from theft or destruction. In the past, physical security was the only protection people needed to be safe. However, with technology, physical security alone is not effective. In information security approach many different layers of security is deployed to achieve what we call “security in layers”. As it is commonly known that nothing is 100 percent secure, information security uses the depth of its layers to achieve the highest form of security. Any weakness in one of these layers will break the security. Physical protection is the first step in the layered approach of information security. If it is nonexistent, or weak, information security will fail (Steinke, 2004.)

2.8.1 Physical Security Threats

Physical security aims to protect against physical threats (Tittel and others, 2003) argue, and following are most common types of physical threats:

- Fire and smoke
- Water (rising/falling)
- Earth movement (earthquakes, landslides, volcanoes)
- Storms (wind, lightning, rain, snow, sleet, ice)
- Sabotage/vandalism
- Explosion/destruction
- Building collapse
- Toxic materials
- Utility loss (power, heating, cooling, air, water)
- Equipment failure
- Personnel loss (strikes, illness, access, transport)

2.8.2 Facility Requirements

The actual facility design can affect the level of physical security available.

2.8.2.1 Entry Points

The following questions should be asked in this point (Hansche and others, 2004, P: 457-458):

- Does the building meet codes for safety requirements?
- Is the building secured at ground level by locked doors, using heavy duty locks?
- How many doors does it have? Where are they located?
- Do doors need to be fire resistant?
- Are trade entrances controlled or wide opened to strangers?
- What type of roof access is needed?
- Does the building have a fire-escape stairs?
- Are there windows at ground level? Are they locked with heavy duty bars?
- Is there sufficient lighting around the entry point which can be easily observed.

2.8.2.2 Infrastructure Support Systems

Infrastructure support systems include power; water/plumbing; and heating, ventilation, and air conditioning. The failure of the support systems may cause physical damage to system hardware or data.

Physical security also includes locations of wiring used to connect parts of the system. For example, cabling, plugs, sockets, and exposed cabling could be broken if left physically accessible (Hansche and others, 2004).

2.8.2.3 Electrical Power

As it is widely known, information systems depend on electricity power, which will affect the business if it faces a disruption. In 2001, the Electric Power Research Institute (ERPI) released a study that said power damage and voltage fluctuations cost the U.S. economy up to $188 billion a year. The report stated that digital firms understand the implications of power to their equipment, so they invest in equipment and generators to protect their systems from unstable power (Hansche and others, 2004, P: 458- 459).

2.8.2.4 Heating, Ventilation, and Air Conditioning (HVAC)

HVAC is defined as a system that provides the processes of comfort heating, ventilation, and/or air conditioning within a space.

The question from the security perspective is, where the location of the main control is, and is it allowed for unauthorized access.

Many HVAC systems are now networked for remote control, monitoring, and maintenance. Hackers have been known to remotely control temperatures. So, controlling remote access should be considered (Hansche and others, 2004, P:461- 462).

2.8.2.5 Internal Sensitive Areas

These areas can include server rooms, data centers, switching centers and users working area, because sensitive information are processed and stored there. Such areas need additional physical protection (Hansche and others, 2004).

2.8.2.6 Portable computing

Each year there are reports from private and public sectors that telling the large number of lost or stolen laptops. These losts could result from forgetting the laptop in a taxi, or theft from a hotel room. Laptop can store large and sensitive information, so, its loss can be very serious (Hansche and others, 2004).

2.8.3 Forms of Physical Access Controls

Physical access controls restrict the entry and exit of personnel, equipment, and media from a building such as an office, data center, or servers' room.

Location security: The physical access controls to the system's elements can include controlled areas, area isolation barriers, entry points in the barriers, and screening measures at that entry points. In addition, trained staff members who work in a restricted area can contribute in providing physical security by challenging unrecognized people.

Support Services and elements: All areas containing system elements must be identified. Physical access controls should address locations of wiring (electricity, networking, telephone ...etc), the electric power service, the air conditioning and heating plant, telephone and data lines, backup media and any other system elements.

Controls effectiveness: Physical access controls effectiveness should be reviewed in each area during normal business hours and in the times when an area unoccupied. Effectiveness depends on both the characteristics of the control devices used and the implementation and operation. Organizations should determine whether intruders can easily defeat the controls, the extent to which strangers are challenged, and the effectiveness of other control procedures. Factors like these modify the effectiveness of physical controls.

Key and combination locks: It is not so difficult to observe an authorized person when he is entering a door locks combination. And it is easy for an intruder to steal a keycard left on a desk if the keycard not carefully controlled.

Corrective actions: If you add an additional barrier, the risk to the areas behind the barrier will be reduced. Enhancing the screening at an entry point can reduce the number of penetrations.

Finally, reorganizing work areas may reduce the number of people who try to access to a restricted area. Intrusion detectors, such as closed-circuit television cameras, motion

detectors, and other devices, can detect intruders in unoccupied spaces (NIST, 1996, P:169 -170).

2.8.4 Information Systems Physical Threats and Controls

The table (2.1) shows some basic threats and controls for information systems.

Table (2. 1): Information Systems Physical Threats and Controls

Risk/Threat	Controls
Loss/theft/destruction poses the following risks: • Loss of sensitive information or trade secrets • Loss of productivity • Loss of revenue	**Loss/theft/destruction controls include** • Physical locks for devices • Marking and tagging devices • Minimize use of location signs • Encryption for sensitive information • Data classification and handing procedures for sensitive information • Insurance • Awareness training • Visible closed circuit television cameras (CCTVs) • Guards • Alarm systems • Routine audits
Unauthorized access poses the following risks: • Loss of sensitive information or trade secrets • Information tampering • Malware • Loss of revenue	**Unauthorized access controls include:** • Locking consoles • Good password practices • Awareness training • Data classification and handing procedures for sensitive information • Minimizing the use of location signs • Visible closed circuit television cameras (CCTVs) • Encryption for sensitive information • Strong authentication and access controls

Source: (Steinke, 2004, P: 3082)

2.8.5 Technical Controls

Technical security involves the use of safeguards incorporated in computer hardware, software, communications, and related devices.

2.8.5.1 Preventive Technical Controls

Preventive technical controls are used to prevent unauthorized personnel or programs from gaining remote access to computing resources. According to (Tipton, 2004, P: 3123-3124) such these controls include:

Access Control Software: The purpose of access control software is to control the usage of data by users, and allowing only registered and authenticated users to gain access to the system and data.

Anti-Virus Software: Viruses can cause processing interruption and loss of data, which lead to loss of productivity. In addition, new viruses are emerging currently about one every 48 hours. It is recommended that anti-virus software be installed on all computers and frequently updated.

Passwords: ID-Password combination is used to authenticate the user against information systems and keeps users accountable for his/her activity on the system.

Currently, dynamic or one-time passwords, which are different for each log-on, are preferred over fixed passwords.

Smart Cards: Smart cards contain a chip with logic functions and information that can be read at a remote terminal to identify a specific user's privileges.

Encryption: Encryption is the transformation of plaintext into cipher text by cryptographic techniques. And it is currently considered to be the only sure way of protecting data from disclosure during network transmissions. Encryption can be implemented with either hardware or software.

Dial-Up Access Control and Callback Systems: Dial-up access to a computer system increases the risk of intrusion by hackers. Currently, the best dial-up access controls use a microcomputer to intercept calls, verify the identity of the caller by checking a username and password in an authorized computing resource.

2.8.5.2 Detective Technical Controls

Detective technical controls warn personnel of violations or attempted violations of preventive technical controls. According to (Tipton, 2004) such controls are:

Audit Trails: An audit trail is a record of system activities that enables the reconstruction and examination of the sequence of events of a transaction, from its beginning to output of final results. Violation reports should be frequently and regularly reviewed by security officers and database owners to identify and investigate successful or unsuccessful unauthorized accesses.

Intrusion Detection Systems: They are considered expert systems because they track users while they are using the system to determine if their activities are normal or not. If not, the user's session can be terminated or a security officer can be called to investigate. Intrusion detection can be especially effective in cases in which intruders are acting as if they are authorized users.

2.9 Telecommunications, Network, and Internet security

Three main topics will be discussed in this section, such topics are Communications and Network Security, Virtual Private Networks (VPNs), and Network Services.

2.9.1 Communications and Network Security

Establishing security on a network involves more than just managing the Operating Security and software. Physical issues must be addressed, such issues include cabling, topology, and technology (Tittel and others, 2003).

2.9.1.1 OSI Model

In order for computers to communicate over a network, they need a common language, such language called protocol. A protocol is a set of rules and restrictions that identify and control the way of data transmission between computers. The International Organization for the Standardization (ISO) developed Open Systems Interconnection (OSI) model for protocols in the early of 1980s. The OSI model divided the networking tasks into seven

layers, each layer responsible for performing specific task. The seven layers are numbered from bottom to top as shown in Figure (2.10).

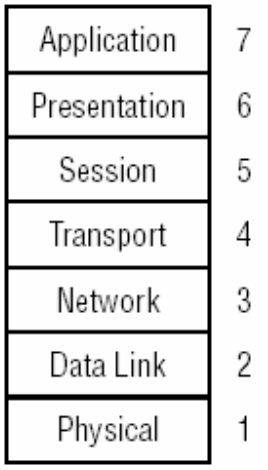


Figure (2. 10): A representation of OSI model
Source: (Tittel and others, 2003, P:73)

The OSI model should be considered by services, applications, and hardware vendors in order to be integrated with others' ones. Protocols based on the OSI model employ a mechanism called encapsulation. As the message is encapsulated at each layer, it grows in size. The process is as follows (Tittel and others, 2003):

1. The Application layer creates a message then passes it to the Presentation layer.
2. The Presentation layer encapsulates the message by adding information at the beginning and the end of the message called header and footer.
3. The message passing down and each layer adding specific information until the message reaches the Physical layer.
4. At the Physical layer, the message is converted into electrical impulses that represent bits and is transmitted over the physical connection.
5. The receiving computer captures the bits from the physical connection and re-creates the message in the Physical layer which in turn strips off its information and sends the message up to the Data Link layer.
6. The Data Link layer strips its information off and sends the message up to the Network layer.

7. This process of de-encapsulation is performed until the message reaches the Application layer which sends the data to the intended software.

Application Layer

The Application layer (layer 7) acts as interface between user applications, network services, or the operating system itself and the protocol stack. It determines whether the destination host in the other part of the network is available and accessible, and ensures that sufficient resources are available to support the requested communications.

Following are application-specific protocols that are found in this layer: HTTP, FTP, SMTP, Telnet, TFTP, POP3, SNMP (Tittel and others, 2003).

Presentation Layer

The Presentation layer (layer 6) is responsible for transforming data received from the Application layer into a format that any system following the OSI model can understand. It imposes standardized structure and formatting rules onto the data. Most file or data formats operate within this layer. Such formats could be for images, video, sound, documents, e-mail, web pages, control sessions, and so on (Tittel and others, 2003).

Session layer

The Session layer (layer 5) is responsible for establishing, maintaining, and terminating communication sessions between two computers. SSL, NFS, SQL, RPC protocols operate within the Session layer:

Communication sessions can operate in one of three different modes:

Simplex: One-direction communication

Half-duplex: Two-way communication, but only one direction can send data at a time

Full-duplex: Two-way communication, in which data can be sent in both directions simultaneously (Tittel and others, 2003).

Transport Layer

The Transport layer (layer 4) is responsible for managing the integrity of a connection and controlling the session. It accepts a Protocol Data Unit (PDU) from the Session layer and

coverts it into a segment. The Transport layer includes mechanisms for segmentation, sequencing, error checking, controlling the flow of data, error correction, and network service optimization, TCP, UDP, SPX protocols operate within the Transport layer (Tittel and others, 2003).

Network Layer

The Network layer (layer 3) is responsible for adding routing information to the data. The Network layer accepts the segment from the Transport layer and adds information to it to create a packet which includes the source and destination IP addresses. Routers are function ate this layer. Routers determine the best logical path for transmission of data packets by using the destination IP address. The following are the routing protocols which located at this layer: ICMP, RIP, OSPF, BGP, IGMP, IP, IPX (Tittel and others, 2003).

Data Link Layer

The Data Link layer (layer 2) is responsible for formatting the packet from the Network layer into the proper format for transmission. The proper format is determined by the hardware and the technology of the network. The packet converted into a properly formatted frame, the hardware source and destination addresses are added to the frame, the frame then sent to the Physical layer for transmission. The following protocols found within the Data Link layer: SLIP, PPP, ARP, RARP, L2F, L2TP, FDDI, ISDN (Tittel and others, 2003)

Physical Layer

The Physical layer (layer 1) accepts the frame from the Data Link layer and converts the frame into bits for transmission over the physical connection medium. It is also responsible for receiving bits from the physical connection medium and converting them back into a frame to be used by the Data Link layer. In the Physical layer there are device drivers that tell the protocol how to use the hardware for transmit and receive bits. Physical layer controls throughput rates, handles synchronization, manages line noise and medium access, and determines whether to use digital or analog signals or light pulses to transmit or receive data over the physical hardware interface (Tittel and others, 2003).

2.9.1.2 Topology

Network topology*:* is the shape of the network or the linked stations.

Node: *is a workstation.*

Bridge: is a connection between two similar networks.

Network protocols: are software implementations providing support for network data transmission.

Following are the common types of network topologies:

The Bus topology: is a popular shape in Local Area Networks (LANs) that offers simple traffic flow between devices (Shim and others, 2000) argue. Authors also added that in bus topology, if a station sends a message to another, the all stations will receive that message. The biggest disadvantage is that a failure in the channel results in loss of the network, and to solve this problem, a redundant channel could be used. Another disadvantage of this topology, it is difficult to isolate faults due to the absence of concentration points. See Figure (2.11)

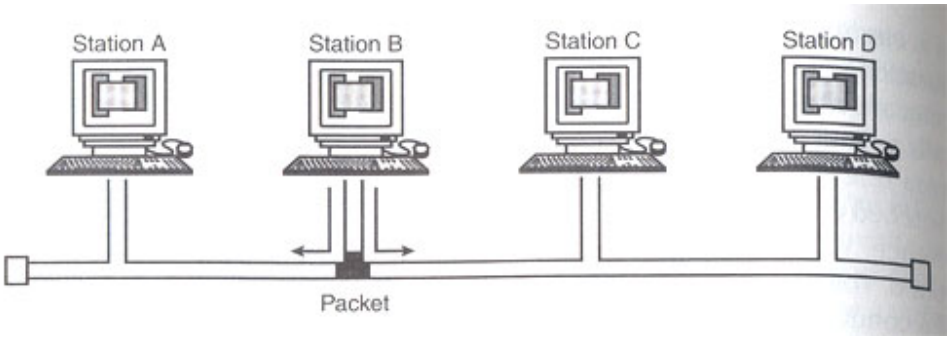


Figure (2. 11): Bus Topology
Source: (Hansche and others, 2004, P:526)

The Star topology: is widely used for data communication systems. It is simple to control the traffic, because it comes from the hub or the center of the star.

Faults will be easily isolated because the use of a central station. If the bottleneck happens at the hub, it could cause serious reliability problems. One way to enhance reliability is to establish a redundant backup of the hub node.

It's easy to identify errors in this system, since each communication must go through the central controller. You can easily expand the network only by running a wire from the new terminal to the host computer (Shim and others, 2000). See Figure (2.12)

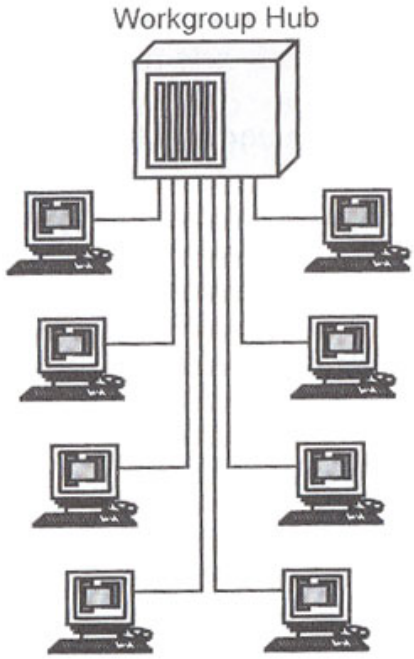


Figure (2. 12): Star Topology
Source: (Hansche and others, 2004, P:527)

The ring topology: in this type of networks, data flows in a circular direction. Every station in the network receives the data and then retransmits it to the next one. One main advantage is that bottlenecks like those in the bus or star networks are relatively uncommon. The primary disadvantage is that the entire network can be lost if the channel between two nodes fails. Establishing a backup channel can usually reduce this problem. A ring network is more reliable and less expensive when there is minimal communication between terminals. With a ring, however, there is greater likelihood of error compared to a star because numerous intervening parties handle data. In light of this, data in a ring system should make an entire circle before being removed from the network (Shim and others, 2000). See Figure (2.13)

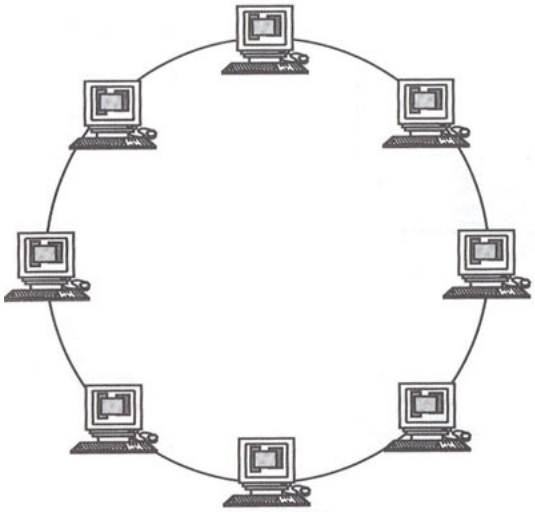


Figure (2. 13): Ring Topology
Source: (Hansche and others, 2004, P:527)

The mesh topology: is very reliable, though complex. Its structure makes it relatively immune to bottlenecks and other failures. The multiplicity of paths makes it relatively easy to route traffic around failed components or busy nodes (Shim and others, 2000). See Figure (2.14).

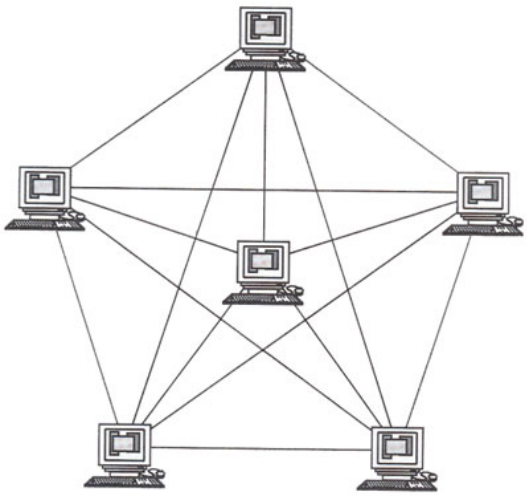


Figure (2. 14): Mesh Topology
Source: (Hansche and others, 2004, P:529)

2.9.1.3 Security Technology and Tools

2.9.1.3.1 Centralized Authentication and Administration Servers

Centralized authentication systems provide an important value to the security administrators. The account management process can be done in one place. So, other systems can use for authentication. It is known as authentication, authorization, and accounting (AAA) servers. As it shown in Figure (2.15), when the user dials in, the Network Access Server (NAS) receives the call and forward it to authentication server for authentication. The authentication server returns the connection parameters, authorization, and protocol information. The NAS then sets up the connection and writes audit record into the database.

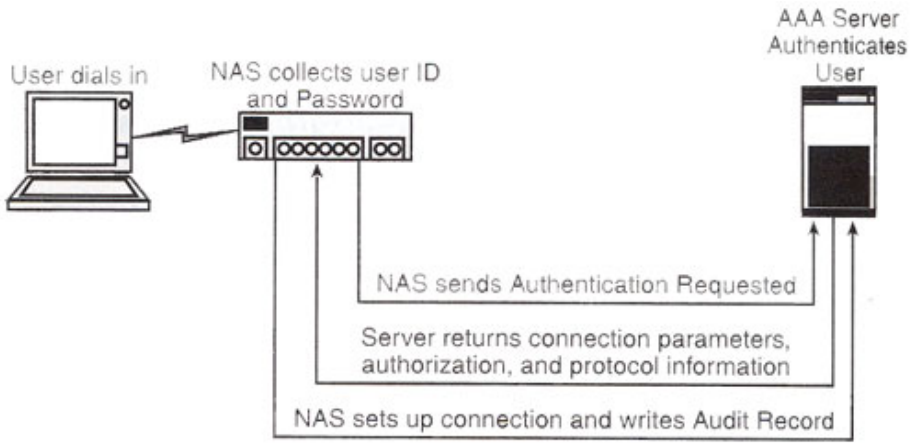


Figure (2. 15): Key Features of a Centralized AAA Service
Source: (Hansche and others, 2004, P: 600)

One of the most popular used AAA servers is the RADIUS.

RADIUS: Remote Authentication Dial-In User Service

Current RADIUS implementations exist for most major platforms as both freeware and commercial implementations. A RADIUS server requires two configurations, one specifying client configuration and one for users. The client configuration file contains the IP addresses of the clients and the shared secret used to authenticate the connections. The user file contains the user ID, password, and authorization parameters.

RADIUS Limitations:

- It is not well suited for host or application authentication.
- It provides no support for system events.

But RADIUS is efficient, flexible, and well supported. (Hansche and others, 2004, P: 599, 603)

2.9.1.3.2 Firewalls and Perimeter Security

(Thorsheim, 2004, P: 769) has identified the firewall as a router that transmits packets between two or more networks with some kind of security filtering applied on top.

Network-Level Firewalls: Packet Filters: Packet filter firewalls controls traffic based on the source and destination IP address of each IP packet and the destination port.

Many packet filter firewalls also allow checking the packets based on the incoming interface. They may also allow control of the IP packet based on the source port, day and time, protocol type.

Packet filter firewalls inspect every IP packet by itself; they do not see IP packets as part of a session. They will let packets through unless there is some restrictions. They also, only check the HEADER of a packet not the DATA part, which means that tunneling a service within another service, will easily bypass a packet filter, for example, running Telnet on port 80 through a firewall where the standard Telnet port 23 is blocked, but HTTP port 80 is open. Because the packet filter only sees source/destination and port number, it will allow it to pass.

Most routers today can be equipped with access lists, controlling IP traffic flowing through the router with various degrees of security.

Using packet filtering usually has little or no impact on throughput. And packet filter firewalls support most TCP/IP-based services.

One reason we don't use packet filter firewalls is, maintaining consistent rules among many different packet filter firewalls is usually considered very difficult (Thorsheim, 2004).

Stateful Inspection Firewalls: Stateful inspection firewalls have the ability to keep track of the state of connections in addition to the packet filtering abilities. By dynamically keeping track of whether a session is being initiated, currently transmitting data, or being closed, the firewall can apply stronger security to the transmission of data. A stateful inspection firewall is capable of understanding the opening, communication, and closing of

sessions. They will not allow a packet to pass if they do not know how to handle the packet. In addition, they can provide an extra level of security by “understanding” the actual contents (the data itself) within packets and sessions, compared to packet filters, and this only applies to specific services, which may vary between products (Thorsheim, 2004).

Application-Level Firewalls: First of all, they provide a high level of security; they support most, if not all, of the usual services that are needed on a day-to-day basis. They understand the protocols at the application layer and, as such, they may block parts of a protocol, for example they could allow FTP to send but not to receive files. They can also detect and block vulnerabilities. The firewall handles all requests made by client, so there is no direct contact between the client and the server. Many application-level firewalls provide caching service for web pages for example, which means faster response times and higher throughput (Thorsheim, 2004).

Perimeter Defense and How Firewalls Fit In: There are statistics showing that internal employees carry out maybe 50 percent of all computer-related crimes, which means the risk not only come from outside the organization. Hackers on the Internet are not allowed access to the internal network, and people or hostile code on the internal network should be prevented from sending sensitive data to the external network. All firewalls and routers connecting the organization to external networks should be properly configured to block services that are considered dangerous. As a general rule, servers and systems that are not in a need to access the internet should not be allowed to. In doing this, viruses and Trojans will not be able to directly establish contact with the system to unauthorized persons on any external network. Security administrators should not allow the servers to be updated directly from the Internet, because this will raise a high security risk to the entire network (Thorsheim, 2004).

Intrusion Detection Systems (IDS): IDS can be a very effective addition to a firewall because it is usually better at logging the contents of the attack compared to a firewall.
It is also easier to create statistics over longer periods of time of hacker activity by using IDS. IDS requires human attention more than a firewall (Thorsheim, 2004, P: 769- 775).

2.9.2 Virtual Private Networks (VPNs):

The VPN is a point-to-point connection between the user's computer and an enterprise server from the user's perspective (Vacca, 2004) argues. The author also added that when the user connecting to a remote network through the Internet or another public network; he/she using VPN network. VPN let all users who use the channel to enjoy the same security and features. VPNs allow remote employees, or branch offices to connect in securely to a server located in the enterprise's LAN by using the networking infrastructure provided by the Internet. Logically, the VPN connection across the Internet operates as a WAN link between the sites.

2.9.2.1 VPN Common Uses

Secure Remote User Access over the Internet.

VPNs provide remote access to enterprise resources over the Internet. This could happen by calling a local ISP Network Access Server (NAS) instead of having a leased-line or making long-distance call to an enterprise. The VPN software creates a virtual private network between the dialup computer and the enterprise VPN server across the Internet using the dialup local connection to the ISP (Vacca, 2004).

Connecting Networks over the Internet.

There are two methods for using VPNs to connect LANs at remote sites according to (Vacca, 2004):

Dedicated Lines to Connect a Branch Office to an Enterprise LAN:

Both the branch office and the enterprise can use a local ISP to connect to the Internet. The two separate established connections and the Internet are then used by the VPN software to create a virtual private network between the two LANs.

Using a Dial-Up Line to Connect a Branch Office to an Enterprise LAN:

The branch office can call the local ISP, rather than having leased-line, or call to an enterprise NAS. Enterprise can call ISP using a dedicated link. The VPN software then uses the connections to the local ISP as shown in Figure (2.16).

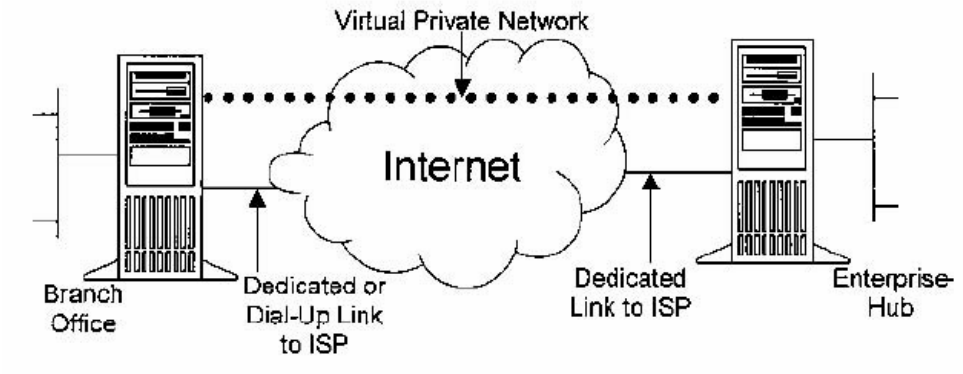


Figure (2. 16): Using a VPN to Connect Two Remote Sites
Source : (Vacca, 2004, P: 830)

The used facilities in connecting the branch office and enterprise offices to the Internet are local in both cases which means a cost savings. It is recommended that the enterprise VPN server be connected to a local ISP with a dedicated line and listening 24 hours per day for incoming VPN traffic (Vacca, 2004).

2.9.2.2 Basic VPN Requirements

A VPN solution should meet all of the following requirements at a minimum:

Address management*:* the solution must assign a client's address on the private net, and must ensure that private addresses are kept private.

Data encryption: data carried on the public network must be rendered unreadable to unauthorized clients on the network.

Key management: the solution must generate and refresh encryption keys for the client and server.

Multi-protocol support: the solution must be able to handle common protocols used in the public network; these include IP, IPX, etc.

User authentication: the solution must verify a user's identity and restrict VPN access to authorized users; in addition, the solution must provide audit and accounting records to show who accessed what information and when (Vacca, 2004).

2.9.3 Network Services

In this topic, E-Mail Security and Network Attacks and Countermeasures will be discussed.

2.9.3.1 E-Mail Security

E-mail is an important and widely used service. The e-mail infrastructure consists of e-mail servers and e-mail clients. E-mail servers using the Simple Mail Transfer Protocol (SMTP) to receive messages from clients, transport them to other servers, and store messages into a user's server-based inbox. E-mail clients retrieve messages from their server-based inboxes using the Post Office Protocol, version 3 (POP3) or Internet Message Access Protocol (IMAP). Clients communicate with e-mail servers using SMTP.

When deploying an SMTP server, it is very important to properly configure authentication for both inbound and outbound mail. Because of SMTP relays mail from sender to intended recipient. However, you have to avoid turning your SMTP server into an open relay (without authentication). Open relays will allow spammers to send out floods of e-mails (Tittel and others, 2003).

E-Mail Security Goals

In fact, basic e-mail is not secure. So security should be added to e-mail in order to achieve some or all of the following objectives (Tittel and others, 2003) argue, authors also mentioned the following as an E-Mail security goals:

- Provide for nonrepudiation
- Restrict access to messages to their intended recipients
- Maintain the integrity of messages
- Authenticate and verify the source of messages
- Verify the delivery of messages
- Classify sensitive content within or attached to messages

Authors also added that the following issues must be addressed in the security policy:

- Acceptable use policies for e-mail
- Access control
- Privacy

- E-mail management
- E-mail backup and retention policies

E-mail Security Solutions

Following are some security solutions that can help to protect e-mail transmission:

Secure Multipurpose Internet Mail Extensions (S/MIME) offers authentication and privacy to e-mail through secured attachments. Public Key Cryptography Standard (PKCS) encryption is used to provide the privacy. Using S/MIME can perform signed messages which provide integrity and sender authentication, and enveloped messages which provide integrity, sender authentication, and confidentiality.

MIME Object Security Services (MOSS) can provide authenticity, confidentiality, integrity, and nonrepudiation for e-mail messages. In order to provide authentication and encryption services, MOSS employs Message Digest 2 (MD2) and MD5 algorithms; Rivest, Shamir, and Adelman (RSA) public key; and Data Encryption Standard (DES).

Privacy Enhanced Mail (PEM) is an e-mail encryption mechanism that provides authentication, integrity, confidentiality, and nonrepudiation. PEM uses RSA, DES, and X.509.

Pretty Good Privacy (PGP) is a public-private key system that uses the IDEA algorithm to encrypt files and e-mail messages (Tittel and others, 2003)..

Many of the vulnerabilities can be reduced or eliminated by using these and other security mechanisms for e-mail and communication transmissions. Digital signatures can help eliminate impersonation. Encryption of messages reduces eavesdropping. And the use of e-mail filters keep spamming and mail bombing to a minimum. Blocking attachments at the e-mail gateway system on your network can ease the threats from malicious attachments (Tittel and others, 2003).

2.9.3.2 Network Attacks and Countermeasures

Eavesdropping: Eavesdropping is the listening to communication traffic for the purpose of recording the data to a storage device or to an extraction. The cracker then can extract many forms of information, such as usernames, passwords, process procedures, data, and so on. Because eavesdropping usually requires physical access to the IT infrastructure, then you

can combat it by maintaining physical access security to prevent unauthorized personnel from accessing your IT infrastructure. In order to greatly reduce the effectiveness and timeliness of eavesdropping, you can use encryption and one-time authentication methods on communication traffic (Tittel and others, 2003).

Impersonation/Masquerading: Impersonation, or masquerading, is the act if you are someone or something you are not in order to gain unauthorized access to a system, this could be happened by capturing the usernames and passwords.
In order to prevent impersonation you can use one-time pads and token authentication systems, Kerberos, and encryption. These solutions can increase the difficulty of extracting authentication credentials from network traffic (Tittel and others, 2003).

Replay Attacks: Replay attacks are using eavesdropping in order to capturing network traffic. They attempt to reestablish a communication session by replaying captured traffic against a system. They can be prevented by using one-time authentication mechanisms and sequenced session identification (Tittel and others, 2003).

Modification Attacks: In this type of attacks, the captured packets are altered and then played against a system. Modified packets are designed to bypass the restrictions of improved authentication mechanisms and session sequencing. Countermeasures to modification replay attacks include the use of digital signature verifications and packet checksum verification (Tittel and others, 2003).

2.10 Business Continuity Planning (BCP)

Business continuity plans main purpose is to prevent interruptions to normal business activity. They are designed to protect critical business processes from failures or disasters, and occurring loss of capital as a result of the unavailability of normal business processes. Business continuity planning is a strategy to minimize the effect of disturbances and to allow for resumption of business processes.
A disruptive event is any intentional or unintentional security infringement that stops normal operations. The aim of BCP is to minimize the effects of a disruptive event on a

company. The primary purpose of business continuity plans are to reduce the risk of financial loss and enhance a company's ability to recover from a disruptive event promptly. The business continuity plan should also help minimize the cost associated with the disruptive event and mitigate the risk associated with it (Krutz and Vines, 2001).

2.10.1 Project Management and Initiation

The project management and initiation phase of BCP considered the base of the other phases, and it involves the following items:

- Establish the need for BCP.
- Obtain top management support and commitment.
- Identify the strategic resources.
- Establish members of the BCP teams.
- Establish the work plan.
- Determine the need for automated data collection tool.
- Prepare a report to management on how BCP will meet its objectives.
- Develop formal meeting schedules.
- Prepare and present status reports.

An important element in the first phase is the top management commitment and support. This may need that the security team to educate the top management on the importance of the BCP.

Nowadays, in some countries like USA, the executives could be held legally responsible for not taking a required care in safeguarding the important information.

After defining the goals and objectives of the BCP, a business continuity planner/coordinator should be hired or identified. This person duty is to make sure that all needed elements of the plan are addressed, and a good preparation and training accomplished for everyone who involved in the BCP process. Moreover, the business continuity planner should serve as a leader for the development team, so, he should be carefully selected to play this role.

Once the process coordinator role has been identified, the next step is to identify the design and development team, following are the team members who should be involved in this process:

- Senior management
- BCP planner/ coordinator
- Recovery Teams
- Business unit representatives
- Crisis management team
- User community
- Systems and network expertise
- Information security department
- Legal representatives

Next step is to establish the project characteristics such as goals, tasks, resources, time schedules, budget estimates, and critical success factors (Hansche and others, 2004, P: 670-673).

2.10.2 Business Impact Assessment (BIA)

The purpose of a BIA is to create a document to be used to help understand the financial or operational impact a disruptive event would have on the business (Krutz and Vines, 2001).

2.10.2.1 BIA goals

-Criticality Prioritization: Every critical business unit process must be identified and prioritized, and the impact of a disruptive event must be evaluated. Obviously, non-time-critical business processes will require a lower priority rating for recovery than time-critical business processes.

-Downtime Estimation: The BIA is used to help estimate what is the longest period of time a critical process can remain interrupted.

-Resource Requirements. The resource requirements for the critical processes are identified considering that the most time-sensitive processes receiving the most resource allocation (Krutz and Vines, 2001).

2.10.2.2 BIA steps

Gathering Assessment Material: The critical business units are identified in this step. Some documents should be prepared in this step; such as business units' relationships and

functional interrelationships of the organization. As the materials are collected and the functional operations of the business are identified, the BIA will examine these business function interdependencies in order to establish a set of priorities between the units and to identify what alternate processing procedures can be utilized (Krutz and Vines, 2001).

The Vulnerability Assessment: It is similar to a Risk Assessment, but it focuses on providing information that is used only for the business continuity plan or disaster recovery plan. A function of a vulnerability assessment is to conduct a loss impact analysis. It will be necessary to define loss criteria both quantitatively and qualitatively.

-Quantitative loss criteria:

- Loss of revenue, capital expenditure, or personal liability resolution
- The operational expenses incurred due to the disruptive event
- Financial loss from resolution of violation of contract agreements
- Financial loss from resolution of violation of regulatory

-Qualitative loss criteria:

- The loss of competitive advantage or market share
- The loss of public confidence or credibility

During the vulnerability assessment, critical support areas must be defined in order to assess the impact of a disruptive event. A critical support area is defined as a business unit or function that must be present to sustain continuity of the business processes, maintain life safety, or avoid public relations embarrassment.

Critical support areas could include the following:

- Telecommunications information technology areas
- Physical infrastructure or plant facilities, transportation services
- Accounting, payroll, transaction processing, customer service, purchasing

Personnel, resources, and services that the critical support areas need to maintain business continuity will also need to be identified (Krutz and Vines, 2001).

Analyzing the Information: Several activities take place during the analysis phase of the BIA, such activities could be documenting required processes, identifying interdependencies, and determining the acceptable interruption period. This section

describes the critical areas requirements in order to keep the revenue stream and maintain transaction processing levels and customer service levels (Krutz and Vines, 2001).

Documentation and Recommendation: A full documentation of all processes, procedures, analysis, and results, and the presentation of recommendations should be reported to the senior management. The report will contain the previously gathered material, list the identified critical support areas, summarize the quantitative and qualitative impact statements, and provide the recommended recovery priorities generated from the analysis (Krutz and Vines, 2001).

2.10.3 Business Continuity Plan Development

In this phase, the BCP team must use the priorities list of concerns raised by the quantitative and qualitative resource prioritization processes and determine the risks that will be included in the business continuity plan, and what is the resources that will be committed to each mitigation task (Tittel and others, 2003).

2.10.3.1 Provisions and Processes

In the provisions and processes task, the BCP team designs the specific procedures and mechanisms that will mitigate the risks considered unacceptable.

There are three categories of assets that must be protected through BCP provisions and processes: people, buildings/facilities, and infrastructure (Tittel and others, 2003).

2.10.3.1.1 People

You must ensure that the people within your organization are safe before, during, and after an emergency. After that you must make provisions to allow your employees to conduct their tasks in a like normal situation. This means that, you should provide the people with all needed resources. Any continuity plan that requires these provisions should include detailed instructions for the BCP team in the event of a disaster. Provisions should be sufficient to feed the operational and support teams for an extended period of time, and it should be maintained in an accessible location and rotated periodically to prevent spoilage (Tittel and others, 2003).

2.10.3.1.2 Buildings/Facilities

In order to carry out critical operations, the businesses may require specialized facilities such as standard office facilities, manufacturing plants, operations centers, warehouses, distribution/logistics centers, and maintenance depots. When performing BIA, those facilities should be identified because they play a critical role in the organization's continued viability. The continuity plan should address two areas for each critical facility:

Hardening provisions: BCP should outline mechanisms and procedures that can be implemented to protect the existing facilities against the defined risks.

Alternate sites: if it's not possible to harden a facility against a risk, the BCP should identify alternate sites where business activities can resume immediately (Tittel and others, 2003).

2.10.3.1.3 Infrastructure

For many businesses, a critical part of infrastructure is the IT and computer systems which comprises a number of servers, workstations, and critical communications links between sites. The BCP must address how these systems will be protected against risks identified during the plan development phase. There are two main methods of providing this protection:

Hardening systems: Protection against risks can be implemented by using computer-safe fire suppression systems and uninterruptible power supplies.

Alternative systems: Business functions may also be protected by introducing redundancy (Tittel and others, 2003).

2.10.4 Plan Approval and Implementation

Plan approval and implementation refers to the following steps (Krutz and Vines, 2001) say:

Approval by senior management

When a disaster strikes, senior management must be able to make informed decisions quickly during the recovery effort, because they have the responsibility for supervision and execution of the plan during a disruptive event, they must have final approval.

Creating an awareness of the plan enterprise-wide

There are three reasons for the organization to disseminate the awareness of the plan between employees, such reasons are:

- Efforts of individuals are very important in the recovery from an event.
- This will emphasize the organization's commitment to its employees.
- Specific training may be required for certain personnel to do their tasks.

Maintenance of the plan, including updating when needed

Business continuity plans often get out of date. The critical business units may be changed if the organizations reorganized. The changing could be in IT infrastructure, including the hardware, software. The reasons for plan maintenance may be administrative because personnel may lose interest or forget, or employee turnover may affect involvement.

Plan maintenance should be continued process to ensure that the plan remains fresh and usable. It's important to build maintenance procedures that centralize responsibility for updates, and create audit procedures that can report regularly on the state of the plan.

It's also important to ensure that multiple versions of the plan do not exist, because it could create confusion when using it (Krutz and Vines, 2001).

2.11 Law, Investigations, and Ethics

Three main topics will be discussed in this section, such topics are Laws, investigations, and Ethics.

2.11.1 Law

It will be very useful for the security professional to have a good understanding of the computer crime laws in his country, or the international laws if he works in an international organization. One of security professional's duties is to interpreting these laws for the top management (Hansche and others, 2004).

2.11.1.1 Categories of Laws

Criminal Law: Laws about individual behavior that violates government laws enacted to protect public (Hansche and others, 2004) argue. Authors also added that criminal law identifies a crime as being a wrong against society; in this case, society is considered the victim. A conviction under criminal law normally results in imprisonment period for the defendant. Some times, it could also result in financial award to the victim as restitution for the crime.

The main purpose of prosecuting under criminal law is punishment for the criminal. The punishment is considered as a deterrent against future crime, but it will not work if it is not strict enough to discourage further criminal activity.

To get someone guilty in a computer crime, a lot of technical evidences and experiences should be available to jury or the judge.

Following are some of the computer-related crimes that can be addressed by criminal law:

- Unauthorized access
- Intellectual property theft
- Theft of computer property
- Invasion of privacy
- Denial of service
- Identity theft

Civil Law: Law about a wrong pointed against an individual or business and resulting a damage or loss. There is no imprisoning under the civil law system, but financial awards as restitution for the loss (Hansche and others, 2004).

Administrative Law: Also known as regulatory law, it establishes the standards of performance for organizations conducting businesses. Violations of these laws can result in financial penalties or imprisonment (Hansche and others, 2004).

Intellectual Property and Privacy Laws

These are other categories of common law, and it is directly related to information. Following are some of these laws:

Patent: It is an official document providing the inventor exclusive rights to an invention. Such document excludes right of the development and use of that invention to the patent holder.

Trademark: It is a name, character, logo, or other symbol identifying a product, service, or organization which and distinguishing them from others ones. Trademark can be registered in the appropriate authority to prevent others from being legally able to use it.

Copyright: It allows the author to protect his right in an idea. The author does not generally have to file for copyright protection, as the law states the copyright comes into forces as soon as the idea is expressed.

Trade secret: Is information that is used, made, or marketed by one having the exclusive legal rights. This means that the organization has the ownership rights to its exclusive use of the information (Hansche and others, 2004).

2.11.1.2 Computer Security, Privacy, and Crime Laws

Appendix (6) contains a list of some laws, regulations, and directives related to computer and information security:

2.11.2 Investigation

Investigating computer crime is known as computer forensics, which is the collecting of information from and about computer systems that is acceptable in a court of law (Krutz and Vines, 2001).

2.11.2.1 Computer Investigation Issues

Because of the nature of information that is stored on the computer, investigating and prosecuting computer criminal cases have unique issues, such as the following:

- Investigation and prosecution time frame is compressed.
- The information is intangible.
- The investigation may interfere with the live operations in an organization.
- Some times, it is difficult to gather the evidence.
- In many instances, an expert or specialist is required.

- Crime locations may be geographically separated, which lead to different jurisdictions (Krutz and Vines, 2001).

2.11.2.2 Evidence

The computer crime evidence may be intangible, and easy to be modified without a trace, so, evidence must be carefully handled and controlled. Following are the major components of the evidence chain that must be followed and protected:

- Location and time evidence was obtained
- Who discovered, secured, and controlled the evidence

To be acceptable in a court of law, evidence must meet the following requirements:

Relevant: The evidence can describe the crime, verify what had occurred, and can fix the crime's time of occurrence.

Legally Permissible: The evidence was obtained in a lawful manner.

Reliability: The evidence has not been modified.

Identification: The evidence is properly identified without changing or damaging.

Preservation: The evidence is not subject to damage or destruction (Krutz and Vines, 2001).

Types of Evidence

Legal evidence can be classified into the following types.

- Best evidence: Original or primary evidence.
- Secondary evidence: An oral description of the evidence contents.
- Direct evidence: Proves or disproves a specific act based on information gathered through the witness's five senses.
- Conclusive evidence: Indubitable; overrides all other evidence.
- Opinions: The following are the two types of opinions:
    - Expert: May offer an opinion based on personal expertise and facts
    - Nonexpert: May give evidence only as to facts
- Circumstantial evidence: Inference of information from other, intermediate, relevant facts (Krutz and Vines, 2001).

2.11.2.3 Conducting the Investigation

Set up a committee of appropriate personnel to deal with the following issues:

- Establishing a prior liaison with law enforcement
- Deciding when and if to bring in law enforcement
- Setting up means of reporting computer crimes
- Put procedures for handling and processing reports of computer crime
- Planning for and conducting investigations
- Involving senior management and the appropriate departments

Ensuring the proper collection of evidence, which includes identification and protection of the various storage media (Krutz and Vines, 2001).

2.11.3 Ethics

Security professionals with important responsibilities are held to a high standard of conduct. The rules that govern personal conduct are collectively known as rules of ethics. Several organizations have recognized the need for standard ethics rules, or codes, and have developed guidelines for ethical behavior.

2.11.3.1 Ethics and the Internet

In January 1989, the Internet Advisory Board (IAB) issued a statement of policy concerning the proper use of the Internet.

The statement is a list of unethical practices which you should not do.

- Seeks to gain unauthorized access to the resources of the Internet
- Disrupts the intended use of the Internet
- Wastes resources (people, capacity, computer) through such actions
- Destroys the integrity of computer-based information
- Compromises the privacy of users (Tittel, 2003, P: 625-626)

2.11.3.2 Ethics Action Plan

The following procedures can help security managers encourage ethical use of the computer within their organizations (Tippett, 2004, P: 3064-3065):

- Developing a corporate guide to computer ethics for the organization.
- Developing a computer ethics policy to complement the computer security policy.
- Adding information about computer ethics to the employee handbook.
- Finding out whether the organization has a business ethics policy, and expanding it to include computer ethics.
- Learning more about computer ethics and spreading what is learned.
- Helping to promote awareness of computer ethics by participating in the computer ethics campaign.
- Making sure the organization has an E-mail privacy policy.
- Making sure employees know what the E-mail policy is.

CHAPTER THREE: RESEARCH METHODOLOGY

3.1 Introduction

This chapter describes the research methodology used for achieving the research goals. It describes the strategy for research design to analyze the usage of Information Technology Management in the IT companies in Palestine. This chapter will also highlight the research population and sample Design. Response rate and respondents representation, review of data collection tool which is the questionnaire, questionnaire validity and reliability, research procedures, and statistical methods used in analyzing data.

3.2 Research Design

The research aims to evaluate to what extent IT companies in Palestine are applying Information Security Management.

The researched topic has divided into ten domains as they are organized by ISO 17799.

The study takes in consideration the way in which international security specialized businesses collecting information about any organization in order to make an assessment for the Information Security situation in such organization.

The questionnaire was used to collect the information, and it was designed like a check list to determine to what extent are Information Security ten Domains are applied in Palestinian IT companies.

3.3 Research Population

The population of this study is the IT companies in Palestine (Gaza Strip, West Bank and Jerusalem) that has a membership in Palestinian IT Association of Companies PITA. The research focused on the managerial level staff in those companies because it discussed the Information security from the management side.

3.3.1 Sample Size

The number of IT companies who has a membership in PITA was 74 when the sample chosen and the research included all those companies in collecting the needed data.

3.3.2 Sampling method and response rate

Table (3.1) shows the sample size, response rate and respondents representation

Table (3. 1): Sample size, response rate and respondents representation

Area	Population *	% of total population	Questionnaires Distributed.	Respondents Rate	Respondents %	% of total responses
Gaza Strip	20	27%	20	14	70%	34.2%
West Bank	49	66.2%	49	25	51%	60.9%
Jerusalem	5	6.8%	5	2	40%	4.9%
Totals	74	100%	74	41	55.4%	100%

* Source of Population distribution: http://www.pita.ps/en/members/List.php (Jan 2007)

3.4 Questionnaire Review

The questionnaire was designed as an assessment tool for the Information Security Management in the IT Companies in Palestine –PITA members-; the first part of the questionnaire contains some questions to collect information about the sample characteristics.

The second part contained the ten Information Security Management domains as designed by ISO 17799. Table (3.2) shows these ten domains and their weights in the questionnaire.

Table (3. 2): distribution of questions to the domains and their weights

Domain	Number of Questions	Weights
Characteristics of respondents	9	13.24%
Security Policy	4	5.88%

Organizational Security	4	5.88%
Asset Classification and Control	3	4.41%
Personnel Security	7	10.29%
Physical and Environmental Security	7	10.29%
Computer and Network Management	13	19.12%
System Access Control	6	8.82%
Systems Development and Maintenance	5	7.35%
Business Continuity Planning	5	7.35%
Compliance	5	7.35%
Total	68	100%

Following are these ten domains and their description:

-Security Policy: the questions of this domain used to determine if the companies have an existing security policy which states the commitment of the top management; and whether that policy has an owner who is responsible for reviewing and updating it.

-Organizational Security: this domain used to determine whether there is a cross functional team responsible for implementing the security controls. and whether the responsibility for the protection of assets are clearly defined; and is there any specialized security advice obtained from outside or not.

-Asset Classification and Control: this domain used to determine if there is an inventory of the important assets associated with information about each asset; and if these assets classified to determine how the information to be protected; and whether existing a procedure for labeling and handling these assets.

-Personnel Security: questions of this domain used to determine the security from the personnel side such as the documentation of the security responsibilities in the job

definitions; and whether the employees asked to sign a confidentiality agreement as part of their employment contract.

-Physical and Environmental Security: this domain intended to determine to what extent the rooms, devices, networking, electricity and other IT facilities are secured by using some security controls such as UPS, electricity generator, and fire alarms.

-Computer and Network Management: this domain used to determine to what extent the computers and networks are secured by asking about the backup procedures, event logs, anti virus and systems updating and upgrading.

-System Access Control: through this domain the usernames, passwords, access rights are assessed, to determine to what extent are the passwords strong, access rights are limited to users in the need to know based.

-Systems Development and Maintenance: this domain used to determine if the validity of input and output, encryption are used. And if some controls for implementation of new software are used.

-Business Continuity Planning: this domain used to determine if there are an emergency planning, and a list of events that could interrupt the business and its results on that business, and if there are plans to restore the business once any of the interruption events happened.

-Compliance: this domain determines whether the contractual requirements were explicitly defined and documented for each information system. And if there are some procedures to ensure compliance with legal restrictions on use of material in respect of which there may be intellectual property rights.

3.5 Questionnaire reliability

The content validity and reliability of the questionnaire was assed by the following ways:

3.5.1 Arbitrating the Questionnaire

The questionnaire has distributed to a group of arbitrators containing three academic members from the Islamic University of Gaza - Faculty of Commerce, and one economical specialist from the Finance Authority. The researcher modified some questions according to the arbitrators' suggestions.

3.5.2 Internal Harmony Testing

The researcher has tested the internal harmony of the questionnaire by calculating the correlation coefficients of each question and the total number of the questions for each domain. The researcher also calculated the correlation coefficients of each domain and the total number of the domains. The correlation coefficients denoted significance at 0.01 level which means a content reliability for what is being measured as shown in table (3.3).

Table (3. 3): Correlation coefficients for internal harmony of the questionnaire

Domain	Correlation coefficient	Significance level
Security Policy	**0.72	.000
Organizational Security	**0.60	.000
Asset Classification and Control	**0.55	.000
Personnel Security	**0.81	.000
Physical and Environmental Security	**0.78	.000
Computer and Network Management	**0.87	.000
System Access Control	**0.89	.000
Systems Development and Maintenance	**0.86	.000
Business Continuity Planning	**0.79	.000
Compliance	**0.81	.000

** (Denotes Significance ate 0.01 level)

3.6 Questionnaire Validity

The researcher used the Alpha-Kronbach test to measure the questionnaire validity. The researcher found Alpha value for every domain and for the total questionnaire. Alpha-Kronbach coefficient was found to be more than 0.7168 for all domains and for the questionnaire as a total, which is very satisfactory for testing the validity of the questionnaire. Table (3.4) shows the results of Alpha-Kronbach test.

Table (3. 4): Alpha-Kronbach coefficients of questionnaire's domains and of the questionnaire as a whole

Domain	Number of questions	Alpha-Kronbach coefficient
Security Policy	4	0.8193
Organizational Security	4	0.7168
Asset Classification and Control	3	0.8691
Personnel Security	7	0.8176
Physical and Environmental Security	7	0.8734
Computer and Network Management	13	0.8943
System Access Control	6	0.8541
Systems Development and Maintenance	5	0.8536
Business Continuity Planning	5	0.9123
Compliance	5	0.8380
All questionnaire questions	59	0.9705

3.7 Research Procedures

3.7.1 Period of the Study

The study was conducted from November 2006 to Feb 2008, but the questionnaire distribution period was from Feb 2007 to Jul 2007.

3.7.2 Place of the Study

The study was applied on the IT companies - PITA members in Gaza Strip, West Bank and Jerusalem.

3.8 Data analysis

The researcher used the email to distribute and collect the questionnaires, all questionnaires considered valid because there were no uncompleted questionnaires. The researcher used the SPSS package to analyze data. The following scale was used in entering the data into SPSS package:

Scale	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
Degree	4	3	2	1	0

3.9 Statistical Methods

The following statistical tests were used to analyze the data and to test the hypothesis:

1- Frequencies, means and percentages to represent the collected data in a meaningful numbers.

2- Pearson correlation factor and Alpha-Kronbach factor to test the reliability and validity of the questionnaire.

3- Sign-test to indicate the significance difference between two independent samples and to prove the hypothesis.

4- Kruskal-Wallis to test the variance between different samples.

CHAPTER FOUR: DATA ANALYSIS AND DISCUSSION

4.1 Introduction

This chapter will be divided in two parts. The first one will describe the respondents' specifications (Sample characteristics) in terms of their qualifications, specialty, experience, title, company age, working field, used operating systems, budget, and address. The second part will contain the analysis of the questionnaire paragraphs and ten domains, and testing the hypothesis.

4.2 Sample Characteristics

4.2.1 Respondents' Qualifications

Table (4. 1): Respondents' Qualifications representation

Qualification	Frequency	Percent
Bachelor	33	80.5
High Education	8	19.5
Total	41	100.0

Most of the respondents are having a bachelor degree (80.5%), while the others (19.5%) having a high education degree, which means that all respondents are educated and having at least bachelor degree, Table (4.1) shows that.

4.2.2 Respondents' Specialty

Table (4. 2): Respondents' Specialty representation

Specialty	Frequency	Percent
Computer Engineering	16	40.0
Computer Science	15	37.5
Business Administration	3	7.5
Other	6	15
Total	40	100.0

We can notice from the results in Table (4.2) that most of the respondents are having a specialty in computer field (77.5%), which is distributed between computer engineering and computer science. The other respondents are having different specialties (22.5%).

4.2.3 Respondents' Experience

Table (4. 3): Respondents' Experience representation

Experience	Frequency	Percent
Two to five years	12	29.3
Six to ten years	13	31.7
More than ten years	16	39.0
Total	41	100.0

It is clear from Table (4.3) that most (70.7%) of the respondents are having not less than six years of experience, while others (29.3%) having not less than two years of experience, this mean that the respondents having a good experience in their working field.

4.2.4 Respondents' Titles

Table (4. 4): Respondents' Title representation

Title	Frequency	Percent
Company Director	19	46.3
Systems Administrator	4	9.8
Database Administrator	2	4.9
Network Administrator	4	9.8
Technical Manager	5	12.2
Other	7	17
Total	41	100.0

From Table (4.4); we can notice that the majority of respondents (83%) are in managerial or administrative posts, while the others (17%) are in different posts.

4.2.5 Companies' Age in IT Field

Table (4. 5): Respondents' company age in IT field

Company age	Frequency	Percent
Less than two years	2	4.9
Two to five years	7	17.1
Six to ten years	13	31.7
More than ten years	19	46.3
Total	41	100.0

Most of respondents' companies (95.1%) are working in IT field for at least two years, while the others (4.9%) are working in IT field for less that two years. Table (4.5) shows these facts.

4.2.6 Companies' Main Working Field

Table (4. 6): Respondents' main working field representation

Company main working field	Frequency	Percent
Suppliers of equipment in computing and telecommunications	19	46.3
Database Building	6	14.6
Application software suppliers	8	19.5
Internet service providers	4	9.8
Professional network services suppliers	1	2.4
Professional Technical Training	3	7.3
Total	41	100.0

Around one halve (46.3%) of respondents are working in supplying equipments of computer and telecommunication field, and around one fifth (19.5) of them are working as application software suppliers, while the other respondents are working in another fields of IT that distributed between database building (14.6%), Internet service providers (9.8%), Professional network services suppliers (2.4%), and Professional Technical Training (7.3%). Table (4.6) shows these facts. This information tells that the Palestinian IT companies are distributed between the different fields of IT.

4.2.7 Used Operating Systems

Table (4. 7): Respondents' used operating systems representation

Operating systems	Frequency	Percent
Windows	20	48.8
Linux/Unix	1	2.4
Windows & Linux/Unix	20	48.8
Total	41	100.0

Around one halve (48.8%) of respondents are using only Windows operating system, and around one halve (48.8%) of them are using two operating systems which is Windows &

Linux/Unix, while only one respondent (2.4%) is using Linux/Unix as the only operating system. Table (4.7) shows these facts.

4.2.8 Security Budget

Table (4. 8): Respondents' Security Budget representation

Budget	Frequency	Percent
Less than 1%	10	24.4
1% to 3%	13	31.7
4% to 5%	7	17.1
More than 5%	11	26.8
Total	41	100.0

Around one third (31.7%) of respondents are specifying one to three percent of their budget to information security management, around one fourth (26.8%) of them are specifying more than five percent to this issue, and around one fourth (24.4%) too specifying less than one percent to the same issue, while the others (17.1) are specifying four to five percent of their budget to information security management. Table (4.8) shows these facts.

4.2.9 Respondents' geographical distribution

Table (4. 9): Respondents' Address representation

Company Address	Frequency	Percent
Gaza Strip	14	34.1
West Bank	20	48.8
Gaza Strip & West Bank	5	12.2
Jerusalem	2	4.9
Total	41	100.0

Most (61%) of respondents are working in West Bank, and around one halve (46.3%) of them are working in Gaza Strip, while the others (4.9%) are working in Jerusalem. This could be normal because the West Bank area is bigger than Gaza Strip. Table (4.9) shows these facts.

4.3 Data analysis and hypothesis testing

4.3.1 Domain One: Security Policy

Table (4. 10): Domain One: Security Policy

#	Question		Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Responses	Mean	%	Sign Test
10	There exists an Information security policy, which is approved by the management and known by all employees.	#	0	3	6	21	11	41	2.98	74.39	.0000
		%	0	7.3	14.6	51.2	26.8				
11	The policy states the management commitment and set out the organizational approach to managing information security.	#	0	2	5	23	11	41	3.05	76.22	.0000
		%	0	4.9	12.2	56.1	26.8				
12	The Security policy has an owner, who is responsible for its maintenance and review according to a defined review process.	#	0	5	9	13	41	41	2.88	71.95	.0001
		%	0	12.2	22	31.7	34.1				
13	The process ensures that a review takes place in response to any changes affecting the basis of the original assessment, example: significant security incidents, new vulnerabilities or changes to organizational or technical infrastructure.	#	0	3	5	15	18	41	3.17	79.27	.0000
		%	0	7.3	12.2	36.6	43.9				
Domain One: Security Policy									3.018	75.46	.000

The results related to domain one (security policy), shown in Table (4.10) denote the following facts:

-In reference to paragraph (10): most of Palestinian IT companies (78%) have an information security policy approved by the management and known by all employees,

while the minority (7.3%) of them do not have such that policy. This is confirmed since the mean of responses to this paragraph is 2.98 with a significance level of 0.0000 for the sign test, which is less than 0.05.

-In reference to paragraph (11): the majority of companies (82.9%) stipulates their commitment to and set out their organizational approach to managing the information security in their policy, while the minority (4.9%) of them do not have the management's commitment stipulated in their policy. This is confirmed since the mean of responses to this paragraph is 3.05 with a significance level of 0.0000 for the sign test, which is less than 0.05.

-In reference to paragraph (12): around two thirds of companies (65.8%) assign a security policy owner responsible for maintenance and review of the security policy according to a defined review process, while the minority of them do not assign a security policy owner. This is due to the fact that the mean of responses to this paragraph is 2.88 with a significance level of 0.0001 for the sign test, which is less than 0.05.

-In reference to paragraph (13): the review process in most of companies (80.5%) ensures that a review takes place in response to any changes affecting the basis of the original assessment, while that is not applied in the other (7.3%) respondents companies. This is confirmed since the mean of responses to this paragraph is 3.17 with a significance level of 0.0000 for the sign test, which is less than 0.05.

Testing Hypothesis 1:

There is a significant effect for written Information Security Policy on the effectiveness of Information Security Management in Palestinian Information Technology companies.

To test this hypothesis, the sign test was used to check the significance of the security Policy domain.

Table (4. 11): Sign test results of the domain "Security Policy"

Domain	Mean	%	Sign Test
Security Policy	3.018	75.46	.0000

The mean of responses on the domain “Security Policy” questions is 3.018 and its percentage weight is 75.46 %, and the value of sign test is 0.0000 which is less than 0.05, this shown in Table (4.11). This confirmed that the security policy in the Palestinian IT companies affecting the effectiveness of Information Security Management in these companies. But it is still need more concern from the top management. This agrees with the study of (Knapp and others, 2006) which stated that the top management support is a key factor of the organization’s security culture and level of policy enforcement.

According to the previous results we can accept the hypothesis “**There is a significant effect for written Information Security Policy on the effectiveness of Information Security Management in Palestinian Information Technology companies**”

4.3.2 Domain Two: Organizational Security

Table (4. 12): Domain Two: Organizational Security

#	Question		Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Responses	Mean	%	Sign Test
14	There is a cross-functional forum of management representatives from relevant parts of the organization to coordinate the implementation of information security controls.	#	0	9	10	18	4	41	2.41	60.37	.0155
		%	0	22	24.4	43.9	9.8				
15	Responsibilities for the protection of individual assets and for carrying out specific security processes were clearly defined.	#	0	8	8	19	6	41	2.56	64.02	.0026
		%	0	19.5	19.5	46.3	14.6				
16	Specialized information security advice is obtained where appropriate.	#	2	13	10	12	4	41	2.07	51.83	.5
		%	4.9	31.7	24.4	29.3	9.8				
17	The implementation of security policy is reviewed independently on regular basis. This is to provide assurance that organizational practices properly reflect the policy, and that it is feasible and effective.	#	3	18	5	10	4	40	1.80	45.12	.1552
		%	7.5	45	12.5	25	10				
Domain Two: Organizational Security									2.226	55.64	.1619

The results related to domain two (Organizational Security), shown in Table (4.12) denote the following facts:

-In reference to paragraph (14): little more than one halve of Palestinian companies (53.7%) have a cross-functional forum of management representatives from relevant parts of the organization to coordinate the implementation of information security controls, while around one fifth (22%) of them do not have such that forum. This is due to the fact that the

mean of responses to this paragraph is 2.41 with a significance level of 0.0155 for the sign test, which is less than 0.05.

-In reference to paragraph (15): little less than two thirds of companies (60.9%) are clearly defined the responsibilities for the protection of individual assets and for carrying out specific security processes, while around fifth (19.5%) of them do not defined that responsibilities. This is due to the fact that the mean of responses to this paragraph is 2.56 with a significance level of 0.0026 for the sign test, which is less than 0.05.

-In reference to paragraph (16): the Palestinian IT companies do not obtain a specialized information security advice as it should be, less than one halve of them only (39.1%) practicing this, while other companies (36.6%) do not obtain a specialized advice. This is confirmed since the mean of responses to this paragraph is 2.07 with a significance level of 0.5 for the sign test, which is above 0.05.

-In reference to paragraph (17): around one third of companies only (35%) reviewing the implementation of the security policy on a regular basis, while around one fifth (52.5%) of them do not practice that. This is due to the fact that the mean of responses to this paragraph is 1.18 with a significance level of 0.1552 for the sign test, which is above 0.05.

Testing Hypothesis 2:

There is a significant effect for Organizational Security structure on the effectiveness of Information Security Management in Palestinian Information Technology companies.

To test this hypothesis, the researcher used the sign test to chek the significance of the Organizational Security domain.

Table (4. 13): Sign test results of the domain Organizational Security

Domain	Mean	%	Sign Test
Organizational Security	2.226	55.64	0.1619

The mean of responses on the domain “Organizational Security” questions is 2.226 and its percentage weight is 55.64%, and the value of sign test is 0.1619 which is above 0.05, Table (4.13) shows that information. This confirmed that the Organizational Security in the Palestinian IT companies does not affect the effectiveness of Information Security

Management in these companies. The researcher refers this to the lack of involving employees and considering them as a major part in the security management process. This agree with (Belsis and Kokolakis, 2005) who argued that most stakeholders lack the required knowledge of Information Systems (IS) security issues that would allow them to play an important role in IS security management.

According to the previous results we cannot accept the hypothesis "**There is a significant effect for Organizational Security structure on the effectiveness of Information Security Management in Palestinian Information Technology companies.**"

4.3.3 Domain Three: Asset Classification and Control

Table (4. 14): Domain Three: Asset Classification and Control

#	Question		Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Responses	Mean	%	Sign Test
18	An inventory or register is maintained with the important assets associated with each information system. (Such register identifies the owner and the location of each asset)	#	0	3	3	22	13	41	3.10	77.44	.0000
		%	0	7.3	7.3	53.7	31.7				
19	There is an Information classification scheme or guideline in place; which will assist in determining how the information is to be handled and protected.	#	1	6	5	17	12	41	2.80	70.12	.0002
		%	2.4	14.6	12.2	41.5	29.3				
20	An appropriate set of procedures are defined for information labeling and handling in accordance with the classification scheme adopted by the organization.	#	1	2	8	21	9	41	2.85	71.34	.0000
		%	2.4	4.9	19.5	51.2	22				
Domain Three: Asset Classification and Control									2.919	72.97	.0000

The results related to domain three (Asset Classification and Control), shown in Table (4.14) denote the following facts:

-In reference to paragraph (18): the majority of Palestinian companies (85.4%) are maintaining an inventory with important assets associated with each information system, while other companies (7.3%) do not maintain such that inventory. This is confirmed since the mean of responses to this paragraph is 3.10 with a significance level of 0.0000 for the sign test, which is less than 0.05.

-In reference to paragraph (19): most of companies (70.8%) are using an information classification scheme or guideline, while other companies (17%) do not use such that scheme. This is confirmed since the mean of responses to this paragraph is 2.80 with a significance level of 0.0002 for the sign test, which is less than 0.05.

-In reference to paragraph (20): most of companies (73.2%) have a set of procedures for information labeling and handling, while other companies (7.3%) do not have such that procedures. This is confirmed since the mean of responses to this paragraph is 2.85 with a significance level of 0.0000 for the sign test, which is less than 0.05.

Testing Hypothesis 3:

There is a significant effect for Asset Classification and Control on the effectiveness of Information Security Management in Palestinian Information Technology companies.

To test this hypothesis, the researcher used the sign test to check the significance of the Asset Classification and Control domain.

Table (4. 15): Sign test results of the domain Asset Classification and Control

Domain	Mean	%	Sign Test
Asset Classification and Control	2.919	72.97	.0000

The mean of responses on the domain questions is 2.919 and its percentage weight is 72.97%, and the value of sign test is 0.0000 which less than 0.05, Table (4.15) shows these information. This confirmed that the Asset Classification and Control in the Palestinian IT companies affecting the effectiveness of Information Security Management in these companies. This agrees with (Fiedler, 2003) who stated that it is import for organizations to have an inventory of all information assets given in an organization in order to protect information assets. The author also added that a classification of the information assets helps to characterize these and assign appropriate protective actions

According to the previous results we can accept the hypothesis **"There is a significant effect for Asset Classification and Control on the effectiveness of Information Security Management in Palestinian Information Technology companies"**

4.3.4 Domain Four: Personnel Security

Table (4. 16): Domain Four: Personnel Security

#	Question		Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Responses	Mean	%	Sign Test
21	Security roles and responsibilities as laid in Organization's information security policy are documented in job definitions.	#	2	4	9	15	11	41	2.71	67.68	.0003
		%	4.9	9.8	22	36.6	26.8				
22	Employees are asked to sign Confidentiality or non-disclosure agreement as a part of their initial terms and conditions of the employment.	#	1	6	10	10	14	41	2.73	68.29	.002
		%	2.4	14.6	24.4	24.4	34.1				
23	All employees of the organization receive appropriate Information Security training and regular updates in organizational policies and procedures.	#	1	11	12	11	6	41	2.24	56.10	.2288
		%	2.4	26.8	29.3	26.8	14.6				
24	A formal reporting procedure exists, to report security incidents through appropriate management channels as quickly as possible.	#	2	7	11	17	4	41	2.34	58.54	.0223
		%	4.9	17.1	26.8	41.5	9.8				
25	A formal reporting procedure or guideline exists for users, to report security weakness in, or threats to, systems or services.	#	1	8	16	11	5	41	2.27	56.71	.1147
		%	2.4	19.5	39	26.8	12.2				
26	There are mechanisms in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored.	#	2	12	12	11	4	41	2.07	51.83	.5
		%	4.9	29.3	29.3	26.8	9.8				

27	There is a formal disciplinary process in place for employees who have violated organizational security policies and procedures.	#	1	5	10	19	6	41	2.59	64.63	.0006
		%	2.4	12.2	24.4	46.3	14.6				
Domain Four: Personnel Security									2.422	60.54	.0003

The results related to domain four (Personnel Security), shown in Table (4.16) denote the following facts:

-In reference to paragraph (21): around two thirds of Palestinian companies (63.4%) have the security roles and responsibilities are documented in job definitions, while other companies (14.7%) do not have documented roles and responsibilities in job definitions. This is due to the fact that the mean of responses to this paragraph is 2.71 with a significance level of 0.0003 for the sign test, which is less than 0.05.

-In reference to paragraph (22): less than two thirds of companies (58.8%) asking the employees to assign a confidentiality agreement as part of their conditions of the employment, while other companies (17%) of them do not ask the employees to assign the same kind of agreements. This is due to the fact that the mean of responses to this paragraph is 2.73 with a significance level of 0.002 for the sign test, which is less than 0.05.

-In reference to paragraph (23): less than one halve of companies (41.4%) conducting training in the information security for all employees and regularly updating they about organizational policies and procedures, while around one third (29.2%) of them do not conduct such that training. This is due to the fact that the mean of responses to this paragraph is 2.24 with a significance level of 0.2288 for the sign test, which is above 0.05.

-In reference to paragraph (24): around one halve of companies (51.3%) have a formal reporting procedure to report security incidents through management channels, while around one fifth (22%) of them do not have such kind of reporting procedure. This is due to the fact that the mean of responses to this paragraph is 2.34 with a significance level of 0.0223 for the sign test, which is less than 0.05.

-In reference to paragraph (25): little more than one third of companies (39%) have a formal reporting procedure or guideline for users to report security weaknesses in systems or threats to services, while around one fifth (21.9%) of them do not such kind of procedure

or guideline. This is due to the fact that the mean of responses to this paragraph is 2.27 with a significance level of 0.1147 for the sign test, which is above 0.05.

-In reference to paragraph (26): around one third of companies (36.6%) have mechanisms to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored, while other companies (34.2%) do not have such kind of mechanisms. This is due to the fact that the mean of responses to this paragraph is 2.07 with a significance level of 0.5 for the sign test, which is above 0.05

-In reference to paragraph (27): little less than two thirds of companies (60.9%) have a formal disciplinary process for employees who have violated organizational security policies and procedures, while other companies (14.6%) do not have such kind of process. This is due to the fact that the mean of responses to this paragraph is 2.59 with a significance level of 0.0006 for the sign test, which is less than 0.05.

Testing Hypothesis 4:

There is a significant effect for applying Personnel Security on the effectiveness of Information Security Management in Palestinian Information Technology companies.

To test this hypothesis, the researcher used the sign test to check the significance of the Personnel Security domain.

Table (4. 17): Sign test results of the domain Personnel Security

Domain	Mean	%	Sign Test
Personnel Security	2.422	60.54	.0003

The mean of responses on the domain "Personnel Security" questions is 2.422 and its percentage weight is 60.54 %, and the value of sign test is 0.0003 which is less than 0.05, Table (4.17) show these information. This confirmed that the Personnel Security in the Palestinian IT companies affecting the effectiveness of Information Security Management in these companies to some extent, but it needs more concern in order to protect the insider abuse of information resources. This agrees with the results of the 2006 Australian Computer Crime and Security Survey that conducted by The Australian High Tech Crime Centre (AHTCC), the Australian Federal Police (AFP) and many other organizations,

which show that 62% of respondents experiencing insider abuse of Internet access, email or computer system resources.

According to the previous results we can accept the hypothesis **"There is a significant effect for applying Personnel Security on the effectiveness of Information Security Management in Palestinian Information Technology companies"**

4.3.5 Domain Five: Physical and Environmental Security

Table (4. 18): Domain Five: Physical and Environmental Security

#	Question		Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Responses	Mean	%	Sign Test
28	The rooms, which have the Information processing service, are locked or have lockable cabinets or safes.	#	0	7	3	16	15	41	2.95	73.78	.0000
		%	0	17.1	7.3	39	36.6				
29	The information is only on need to know basis, which means there exists some security controls for third parties or for personnel working in secure area.	#	0	3	6	16	16	41	3.10	77.44	.0000
		%	0	7.3	14.6	39	39				
30	The equipment is protected from power failures by using permanence of power supplies such as multiple feeds, UPS, backup generator etc.	#	0	4	2	14	21	41	3.27	81.71	.0000
		%	0	9.8	4.9	34.1	51.2				
31	The power and telecommunications cable carrying data or supporting information services are protected from interception or damage.	#	0	4	1	16	19	40	3.17	79.27	.0000
		%	0	10	2.5	40	47.5				
32	The equipment is maintained as per the supplier's recommended service intervals and specifications.	#	0	2	6	20	13	41	3.07	76.83	.0000
		%	0	4.9	14.6	48.8	31.7				
33	Disposal storage device containing sensitive information are physically destroyed or securely over written.	#	0	3	8	12	18	41	3.10	77.44	.0000
		%	0	7.3	19.5	29.3	43.9				
34	Automatic computer screen locking facility is enabled. This would lock the screen when the computer is left unattended for a period	#	0	3	8	19	11	41	2.93	73.17	.0000
		%	0	7.3	19.5	46.3	26.8				
Domain Five: Physical and Environmental Security									3.115	77.89	.0000

The results related to domain five (Physical and Environmental Security), shown in Table (4.18) denote the following facts:

-In reference to paragraph (28): most of Palestinian companies (75.6%) have lockable rooms and cabinets to save the information processing services, while other companies (17.1%) do not have lockable rooms and cabinets. This is confirmed since the mean of responses to this paragraph is 2.95 with a significance level of 0.0000 for the sign test, which is less than 0.05.

-In reference to paragraph (29): most of companies (78%) are dealing with the information on the basis of "only on need to know", while other companies (7.3%) do not deal with the information upon that basis. This is confirmed since the mean of responses to this paragraph is 3.1 with a significance level of 0.0000 for the sign test, which is less than 0.05.

-In reference to paragraph (30): majority of companies (85.6%) using permanence of power supplies to protect the equipment, while other companies (9.8%) do not use the same power supplies. This is confirmed since the mean of responses to this paragraph is 3.27 with a significance level of 0.0000 for the sign test, which is less than 0.05.

-In reference to paragraph (31): the power and telecommunications cables are protected from interception or damage by majority of companies (87%), while other companies (10%) do not protect their cables. This is confirmed since the mean of responses to this paragraph is 3.17 with a significance level of 0.0000 for the sign test, which is less than 0.05.

-In reference to paragraph (32): majority of companies (80.5%) maintaining the equipment as per supplier's recommended intervals and specifications, while other companies (4.9%) do not practice the same maintenance. This is confirmed since the mean of responses to this paragraph is 3.07 with a significance level of 0.0000 for the sign test, which is less than 0.05.

-In reference to paragraph (33): most of companies (73.2%) destroying disposable storage devices or overwriting it before throwing it away, while other companies (7.3%) do not practice the same thing. This is confirmed since the mean of responses to this paragraph is 3.10 with a significance level of 0.0000 for the sign test, which is less than 0.05.

-In reference to paragraph (34): most of companies (73.1%) enable an automatic computer screen locking facilities to lock the screen when the computer is left unused for a certain period of time, while other companies (7.3%) do not use such kind of facilities. This is confirmed since the mean of responses to this paragraph is 2.93 with a significance level of 0.0000 for the sign test, which is less than 0.05.

Testing Hypothesis 5:

There is a significant effect for applying Physical and Environmental Security on the effectiveness of Information Security Management in Palestinian Information Technology companies.

To test this hypothesis, the researcher used the sign test to check the significance of the Physical and Environmental Security domain.

Table (4. 19): Sign test results of the domain Physical and Environmental Security

Domain	Mean	%	Sign Test
Physical and Environmental Security	3.115	77.89	.0000

The mean of responses on the domain "Physical and Environmental Security" questions is 3.115 and its percentage weight is 77.89 %, and the value of sign test is 0.0000 which is less than 0.05. Table (4.19) shows this information. This confirmed that the Physical and Environmental Security in the Palestinian IT companies affecting the effectiveness of Information Security Management in these companies. This agrees with (Steinke, 2004) who stated that if the physical integrity of one computers in an organization is compromised, information security could be at risk. The author also added that if someone were to gain unauthorized physical access to a computer, he/she could also gain access to all of the information on that computer and possibly any other resource that computer is connected to.

According to the previous results we can accept the hypothesis **"There is a significant effect for applying Physical and Environmental Security on the effectiveness of Information Security Management in Palestinian Information Technology companies".**

4.3.6 Domain Six: Computer and Network Management

Table (4. 20): Domain Six: Computer and Network Management

#	Question		Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Responses	Mean	%	Sign Test
35	The Security Policy has identified any Operating procedures such as Back-up, Equipment maintenance etc.,	#	0	3	1	17	20	41	3.32	82.93	.0000
		%	0	7.3	2.4	41.5	48.8				
36	Audit logs are maintained for any change made to the production programs.	#	0	8	6	16	11	41	2.73	68.29	.0011
		%	0	19.5	14.6	39	26.8				
37	There is an Incident Management procedure exists to handle security incidents.	#	1	11	9	15	5	41	2.29	57.32	.1079
		%	2.4	26.8	22	36.6	12				
38	Duties and areas of responsibility are separated in order to reduce opportunities for unauthorized modification or misuse of information or services.	#	0	5	6	18	12	41	2.90	72.56	.0000
		%	0	12.2	14.6	43.9	29.3				
39	The capacity demands are monitored and projections of future capacity requirements are made. Example: Monitoring Hard disk space, RAM, CPU on critical servers.	#	0	4	4	21	12	41	3.00	75.00	.0000
		%	0	9.8	9.8	51.2	29.3				
40	System acceptance criteria are established for new information systems, upgrades and new versions and suitable tests were carried out prior to acceptance.	#	0	3	5	21	12	41	3.02	75.61	.0000
		%	0	7.3	12.2	51.2	29.3				
41	The security policy addresses software licensing issues such as prohibiting usage of unauthorized software.	#	4	6	12	13	6	41	2.27	56.71	.0686
		%	9.8	14.6	29.3	31.7	14.6				

#	Question		Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Responses	Mean	%	Sign Test
42	Antivirus software is installed on the computers to check and isolate or remove any viruses from computer and media and this software signature is updated on a regular basis to check any latest viruses.	#	1	0	0	15	25	41	3.54	88.41	.0000
		%	2.4	0	0	36.6	61				
43	Back-up of essential business information such as production server, critical network components, configuration backup etc., were taken regularly.	#	1	0	0	12	28	41	3.61	90.24	.0000
		%	2.4	0	0	29.3	68.3				
44	Faults are reported and well managed. This includes corrective action being taken.	#	0	3	5	21	12	41	3.02	75.61	.0000
		%	0	7.3	12.2	51.2	29.3				
45	Effective operational controls such as separate network were established where necessary in order to secure the network.	#	1	3	4	18	15	41	3.05	76.22	.0000
		%	2.4	7.3	9.8	43.9	36.6				
46	There is a policy in place for the acceptable use of electronic mail.	#	1	2	7	13	18	41	3.10	77.44	.0000
		%	2.4	4.9	17.1	31.7	43.9				
47	There are some controls in place to protect the integrity of such information publicly available from any unauthorized access.(such as firewalls)	#	0	3	0	18	19	40	3.24	81	.0000
		%	0	7.5	0	45	47.5				
Domain Six: Computer and Network Management									3.013	75.32	.0000

The results related to domain six (Computer and Network Management), shown in Table (4.20) denote the following facts:

-In reference to paragraph (35): security policy in majority of Palestinian IT companies (90.3%) has identified some operating procedures such as back-up and equipment maintenance, while other companies (7.3%) do not have such procedures. This is confirmed since the mean of responses to this paragraph is 3.32 with a significance level of 0.0000 for the sign test, which is less than 0.05.

-In reference to paragraph (36): around two thirds of companies (65.8%) maintain an audit log for any changes to the production programs, while around one fifth (19.5%) of them do not maintain such kind of audit logs. This is due to the fact that the mean of responses to this paragraph is 2.73 with a significance level of 0.0011 for the sign test, which is less than 0.05.

-In reference to paragraph (37): around halve of companies (48.6%) have an incident management procedure to handle security incidents, while around one third of companies (29.2%) do not have such kind of procedure. This is due to the fact that the mean of responses to this paragraph is 2.29 with a significance level of 0.1079 for the sign test, which is above 0.05.

-In reference to paragraph (38): duties and areas of responsibility in most of companies (73.2%) are separated in order to reduce opportunities for unauthorized modification or misuse of information services, while other companies (12.2%) do not separate the duties and areas of responsibilities. This is confirmed since the mean of responses to this paragraph is 2.90 with a significance level of 0.0000 for the sign test, which is less than 0.05.

-In reference to paragraph (39): capacity demands are monitored and projections of future capacity requirements are made in majority of companies (80.5%), while other companies (9.8%) do not practice such kind of monitoring and projection. This is confirmed since the mean of responses to this paragraph is 3.00 with a significance level of 0.0000 for the sign test, which is less than 0.05.

-In reference to paragraph (40): majority of companies (80.5%) have system acceptance criteria for new information systems, upgrades and new versions, while other companies

(7.3%) do not have such kind of criteria. This is confirmed since the mean of responses to this paragraph is 3.02 with a significance level of 0.0000 for the sign test, which is less than 0.05.

-In reference to paragraph (41): the security policy in less than one halve of companies (46.3%) addresses software licensing issues such as prohibiting usage of unauthorized software, while this does not addressed in other companies' (24.4%) security policies. This is due to the fact that the mean of responses to this paragraph is 2.27 with a significance level of 0.0686 for the sign test, which is above 0.05.

-In reference to paragraph (42): high majority of companies (97.6%) use antivirus software and updating it on a regular basis in order to check any new viruses, while other companies (2.4%) do not use an updated antivirus. This is confirmed since the mean of responses to this paragraph is 3.54 with a significance level of 0.0000 for the sign test, which is less than 0.05.

-In reference to paragraph (43): high majority of companies (97.6%) too taking a backup of their essential business information in a regular basis, while other companies (2.4%) do not practice such kind of backup. This is confirmed since the mean of responses to this paragraph is 3.61 with a significance level of 0.0000 for the sign test, which is less than 0.05.

-In reference to paragraph (44): majority of companies (80.5%) report the faults and manage it well, while other companies (7.3%) do not report the faults. This is confirmed since the mean of responses to this paragraph is 3.02 with a significance level of 0.0000 for the sign test, which is less than 0.05.

-In reference to paragraph (45): majority of companies (80.5%) established effective operational controls in order to secure the network, while other companies (9.7%) do not establish such kind of controls. This is confirmed since the mean of responses to this paragraph is 3.05 with a significance level of 0.0000 for the sign test, which is less than 0.05.

-In reference to paragraph (46): most of companies (75.6%) have a policy for the acceptable use of electronic mail, while other companies (7.3%) do not have such kind of policy. This is confirmed since the mean of responses to this paragraph is 3.10 with a significance level of 0.0000 for the sign test, which is less than 0.05.

-In reference to paragraph (47): high majority of companies (92.5%) applying some controls to protect the integrity of publicly available information from any unauthorized access, while other companies (7.5%) do not apply such kind of controls. This is confirmed since the mean of responses to this paragraph is 3.24 with a significance level of 0.0000 for the sign test, which is less than 0.05.

Testing Hypothesis 6:

There is a significant effect for Computer and Network Management on the effectiveness of Information Security Management in Palestinian Information Technology companies.

To test this hypothesis, the researcher used the sign test to check the significance of the Computer and Network Management domain.

Table (4. 21): Sign test results of the domain Computer and Network Management

Domain	Mean	%	Sign Test
Computer and Network Management	3.013	75.32	.0000

The mean of responses on the domain "Computer and Network Management" questions is 3.013 and its percentage weight is 75.32 %, and the value of sign test is 0.0000 which is less than 0.05, Table (4.21) show this information. This confirmed that the Computer and Network Management in the Palestinian IT companies affecting the effectiveness of Information Security Management in these companies.

According to the previous results we can accept the hypothesis **"There is a significant effect for Computer and Network Management on the effectiveness of Information Security Management in Palestinian Information Technology companies"**

4.3.7 Domain Seven: System Access Control

Table (4. 22): Domain Seven: System Access Control

#	Question		Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Responses	Mean	%	Sign Test
48	The access control policy does address the rules and rights for each user or a group of users.	#	0	2	4	17	17	40	3.15	78.66	.0000
		%	0	5	10	42.5	42.5				
49	There exists a process to review user access rights at regular intervals.	#	1	4	9	17	10	41	2.76	68.90	.0001
		%	2.4	9.8	22	41.5	24.4				
50	There are some guidelines in place to guide users in selecting and maintaining secure passwords.	#	1	4	8	18	10	41	2.78	69.51	.0000
		%	2.4	9.8	19.5	43.9	24.4				
51	A unique identifier is provided to every user such as operators, system administrators and all other staff including technical.	#	1	1	5	17	17	41	3.17	79.27	.0000
		%	2.4	2.4	12.2	41.5	41.5				
52	The sensitive systems are provided with isolated computing environment such as running on a dedicated computer, share resources only with trusted application systems.	#	1	3	3	19	15	41	3.07	76.83	.0000
		%	2.4	7.3	7.3	46.3	36.6				
53	An audit logs recording security relevant events are produced and kept for an agreed period to assist in future investigations and access control monitoring.	#	0	8	12	12	9	41	2.54	63.41	.0129
		%	0	19.5	29.3	29.3	22				
Domain Seven: System Access Control									2.924	73.11	.0000

The results related to domain seven (System Access Control), shown in Table (4.22) denote the following facts:

-In reference to paragraph (48): the access control policy of majority of Palestinian IT companies (85%) addresses the rules and rights for each user and group of users, while other companies policies (5%) does not reflect that rules and rights. This is confirmed since the mean of responses to this paragraph is 3.15 with a significance level of 0.0000 for the sign test, which is less than 0.05.
-In reference to paragraph (49): around two thirds of companies (65.9%) have a process to review user access rights at regular intervals, while other companies (12.2%) do not have such kind of process. This is confirmed since the mean of responses to this paragraph is 2.76 with a significance level of 0.0000 for the sign test, which is less than 0.05.

-In reference to paragraph (50): around two thirds of companies (68.3%) have some guidelines to guide users in selecting and maintaining secure passwords, while other companies (12.2%) do not have such kind of theses guidelines. This is due to the fact that the mean of responses to this paragraph is 2.78 with a significance level of 0.0000 for the sign test, which is less than 0.05.
-In reference to paragraph (51): majority of companies (83%) providing a unique identifier to every user such as operators, system administrators and all other staff including technical, while other companies (4.8%) do not do the same thing. This is confirmed since the mean of responses to this paragraph is 3.17 with a significance level of 0.0000 for the sign test, which is less than 0.05.
-In reference to paragraph (52): the sensitive systems in majority of companies (82.9%) are provided with isolated computing environment, while other companies (9.7%) do not follow the same technique. This is confirmed since the mean of responses to this paragraph is 3.07 with a significance level of 0.0000 for the sign test, which is less than 0.05.
-In reference to paragraph (53): an audit log recording security relevant events are produced by around one halve of companies (51.3%); such log kept for agreed period to assist in future investigations and access control monitoring, while other companies (19.5%) do not produce such kind of these logs. This is due to the fact that the mean of responses to this paragraph is 2.54 with a significance level of 0.0129 for the sign test, which is less than 0.05.

Testing Hypothesis 7:

There is a significant effect for System Access Control on the effectiveness of Information Security Management in Palestinian Information technology companies.

To test this hypothesis, the researcher used the sign test to check the significance of the System Access Control domain.

Table (4. 23): Sign test results of the domain System Access Control

Domain	Mean	%	Sign Test
System Access Control	2.924	73.11	.0000

The results in Table (4.23) show that the mean of responses on the domain "System Access Control" questions is 2.924 and its percentage weight is 73.11%, and the value of sign test is 0.0000 which is less than 0.05. This confirmed that the System Access Control in the Palestinian IT companies affecting the effectiveness of Information Security Management in these companies. This agrees with Hong and others (2003) that security is to combine systems, operations, and internal controls to ensure integrity and confidentiality of data and operation procedures in an organization. Authors also added that with the arrival of information technology, users' roles in information systems have evolved from IT specialists for access information facilities, to non-IT personnel for regular operations, to unspecified individuals from outside.

According to the previous results we can accept the hypothesis **"There is a significant effect for System Access Control on the effectiveness of Information Security Management in Palestinian Information technology companies".**

4.3.8 Domain Eight: Systems Development and Maintenance

Table (4. 24): Domain Eight: Systems Development and Maintenance

#	Question		Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Responses	Mean	%	Sign Test
54	The data input to application system is validated to ensure that it is correct and appropriate.	#	0	3	2	21	15	41	3.17	79.27	.0000
		%	0	7.3	4.9	51.2	36.6				
55	The data output of application system is validated to ensure that the processing of stored information is correct and appropriate to circumstances.	#	0	2	4	18	17	41	3.22	80.49	.0000
		%	0	4.9	9.8	43.9	41.5				
56	Encryption techniques were used to protect the data.	#	2	8	10	15	6	41	2.37	59.15	.0362
		%	4.9	19.5	24.4	36.6	14.6				
57	There are some controls in place for the implementation of software on operational systems. This is to minimize the risk of corruption of operational systems.	#	0	2	3	24	12	41	3.12	78.05	.0000
		%	0	4.9	7.3	58.5	29.3				
58	There are strict control procedures in place over implementation of changes to the information system. This is to minimize the corruption of information system.	#	1	4	4	17	15	41	3.00	75.00	.0000
		%	2.4	9.8	9.8	41.5	36.6				
Domain Eight: Systems Development and Maintenance									2.976	74.39	.0000

The results related to domain eight (Systems Development and Maintenance), shown in Table (4.24) denote the following facts:

-In reference to paragraph (54): majority of Palestinian IT companies (87.8%) validating the data input to application system to ensure that it is correct and appropriate, while other

companies (7.3%) do not use such kind of validation. This is confirmed since the mean of responses to this paragraph is 3.17 with a significance level of 0.0000 for the sign test, which is less than 0.05.

-In reference to paragraph (55): majority of companies (85.4%) validating the data output of applications system to ensure that the processing of stored information is correct and appropriate, while other companies (4.9%) do not use such kind of validation.

-In reference to paragraph (56): around one halve of companies (51.2%) using encryption techniques to protect the data, while around one fourth of tem (24.4%) do not use such kind of techniques. This is due to the fact that the mean of responses to this paragraph is 2.37 with a significance level of 0.0362 for the sign test, which is less than 0.05.

-In reference to paragraph (57): majority of companies (87.8%) using some controls for the implementation of software on operational systems, while other companies (4.9%) do not use such kind of controls. This is confirmed since the mean of responses to this paragraph is 3.12 with a significance level of 0.0000 for the sign test, which is less than 0.05.

-In reference to paragraph (58): most of companies (78.1%) have strict control procedures for implementation of changes to the information systems, while other companies (12.2%) do not use such kind of procedures. This is confirmed since the mean of responses to this paragraph is 3.00 with a significance level of 0.0000 for the sign test, which is less than 0.05.

Testing Hypothesis 8:

There is a significant effect for Systems Development and Maintenance on the effectiveness of Information Security Management in Palestinian Information Technology companies.

To test this hypothesis, the researcher used the sign test to check the significance of the Systems Development and Maintenance domain.

Table (4. 25): Sign test results of the domain Systems Development and Maintenance

Domain	Mean	%	Sign Test
Systems Development and Maintenance	2.976	74.39	.0000

The mean of responses on the domain “Systems Development and Maintenance” questions is 2.976 and its percentage weight is 74.39 %, and the value of sign test is 0.0000 which is less than 0.05, this is shown in Table (4.25). This confirmed that the Systems Development and Maintenance in the Palestinian IT companies affecting the effectiveness of Information Security Management in these companies. This agrees with (Grance, Hash, and Stevens, 2004) whom stated that including security early in the information system development life cycle (SDLC) will usually result in less expensive and more effective security than adding it to an operational system.

According to the previous results we can accept the hypothesis **“There is a significant effect for Systems Development and Maintenance on the effectiveness of Information Security Management in Palestinian Information Technology companies”.**

4.3.9 Domain Nine: Business Continuity Planning

Table (4. 26): Domain Nine: Business Continuity Planning

#	Question		Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Responses	Mean	%	Sign Test
59	There is a managed process in place for developing and maintaining business continuity throughout the organization.	#	0	3	10	19	9	41	2.83	70.73	.0000
		%	0	7.3	24.4	46.3	22				
60	The events that could cause interruptions to business process were identified example: equipment failure, flood and fire.	#	1	4	11	18	7	41	2.63	65.85	.0002
		%	2.4	9.8	26.8	43.9	17.1				
61	Plans were developed to restore business operations within the required time frame following an interruption or failure to business process.	#	1	6	8	16	10	41	2.68	67.07	.0008
		%	2.4	14.6	19.5	39	24.4				
62	There is a single framework of business continuity plan, this framework is maintained to ensure that all plans are consistent and identify priorities for testing and maintenance. Such framework identifies individuals responsible for executing each component of the plan.	#	2	6	6	18	9	41	2.63	65.85	.0011
		%	4.9	14.6	14.6	43.9	22				
63	Business continuity plans are tested regularly to ensure that they are up to date and effective.	#	1	5	12	19	4	41	2.49	62.20	.0014
		%	2.4	12.2	29.3	46.3	9.8				
Domain Nine: Business Continuity Planning									2.654	66.34	.0002

The results related to domain nine (Business Continuity Planning), shown in Table (4.26) denote the following facts:

-In reference to paragraph (59): around two thirds of Palestinian IT companies (68.3%) have a managed process for developing and maintaining business continuity throughout the organization, while other companies (7.3%) do not have such kind of process. This is due to the fact that the mean of responses to this paragraph is 2.83 with a significance level of 0.0000 for the sign test, which is less than 0.05.

-In reference to paragraph (60): the events that could cause interruptions to business process are identified in less than two thirds of companies (61%), while other companies (12.2%) do not identify such kind of events. This is due to the fact that the mean of responses to this paragraph is 2.63 with a significance level of 0.0002 for the sign test, which is less than 0.05.

-In reference to paragraph (61): less than two thirds of companies (63.4%) developed plans to restore business operations within required time frame following an interruption or failure to business process, while other companies (17%) do not develop such kind of plans. This is due to the fact that the mean of responses to this paragraph is 2.68 with a significance level of 0.0008 for the sign test, which is less than 0.05.

-In reference to paragraph (62): around two thirds of companies (65.9%) have a single framework of business continuity plan which is maintained to ensure that all plans are consistent and identify priorities for testing and maintenance, while other companies (19.5%) do not have such kind of framework. This is due to the fact that the mean of responses to this paragraph is 2.63 with a significance level of 0.0011 for the sign test, which is less than 0.05.

-In reference to paragraph (63): little more than one halve of companies (56.1%) testing their business continuity plans regularly to ensure that they are up to date and effective, while other companies (14.6%) do not test their plans regularly. This is due to the fact that the mean of responses to this paragraph is 2.49 with a significance level of 0.0014 for the sign test, which is less than 0.05.

Testing Hypothesis 9:

There is a significant effect for Business Continuity Planning on the effectiveness of Information Security Management in Palestinian Information Technology companies.

To test this hypothesis, the researcher used the sign test to check the significance of the Business Continuity Planning domain.

Table (4. 27): Sign test results of the domain Business Continuity Planning

Domain	Mean	%	Sign Test
Business Continuity Planning	2.654	66.34	.0001

The results in Table (4.27) show that the mean of responses on the domain "Business Continuity Planning" questions is 2.654 and its percentage weight is 66.34%, and the value of sign test is 0.0003 which is less than 0.05. This confirmed that the Business Continuity Planning in the Palestinian IT companies affecting the effectiveness of Information Security Management in these companies to some extent. This agrees, to some extent with the study of (Botha and Solms, 2004) which stated that the small and medium organizations could prove difficult of developing a business continuity plan.

According to the previous results we can accept the hypothesis "**There is a significant effect for Business Continuity Planning on the effectiveness of Information Security Management in Palestinian Information Technology companies**"

4.3.10 Domain Ten: Compliance

Table (4. 28): Domain Ten: Compliance

#	Question		Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree	Responses	Mean	%	Sign Test
64	All relevant statutory, regulatory and contractual requirements were explicitly defined and documented for each information system. Specific controls and individual responsibilities to meet these requirements were defined and documented.	#	0	5	16	15	5	41	2.49	62.20	.002
		%	0	12.2	39	36.6	12.2				
65	There exist and well implemented some procedures to ensure compliance with legal restrictions on use of material in respect of which there may be intellectual property rights (copyright, design rights, trade marks).	#	0	8	14	14	5	41	2.39	59.76	.0271
		%	0	19.5	34.1	34.1	12.2				
66	There is a management structure and control in place to protect data and privacy of personal information.	#	0	3	6	19	12	40	2.93	73.17	.0000
		%	0	7.5	15	47.5	30				
67	All areas within the organization are considered for regular review to ensure compliance with security policy, standards and procedures.	#	1	6	10	18	6	41	2.54	63.41	.002
		%	2.4	14.6	24.4	43.9	14.6				
68	Access to system audit tools such as software or data files are protected to prevent any possible misuse or compromise.	#	0	2	7	19	13	41	3.05	76.22	.0000
		%	0	4.9	17.1	46.3	31.7				
Domain Ten: Compliance									2.690	67.26	.0003

The results related to domain ten (Compliance), shown in Table (4.28) denote the following facts:

-In reference to paragraph (64): little less than one halve of Palestinian IT companies (48.8%) defined and documented all relevant statutory, regulatory and contractual requirements for each information system, while other companies (12.2%) do not defined and document such kind of requirements. This is due to the fact that the mean of responses to this paragraph is 2.49 with a significance level of 0.002 for the sign test, which is less than 0.05.

-In reference to paragraph (65): less than one halve of companies (46.3%) have and well implement some procedures to ensure compliance with legal restrictions on use of material in respect of which there may be intellectual property rights, while other companies (19.5%) do not have such kind of procedures. This is due to the fact that the mean of responses to this paragraph is 2.39 with a significance level of 0.0271 for the sign test, which is less than 0.05.

-In reference to paragraph (66): most of companies (77.5%) have a management structures and controls to protect data and privacy of personal information, while other companies (7.5%) do not have such kind of structure and control. This is confirmed since the mean of responses to this paragraph is 2.93 with a significance level of 0.0000 for the sign test, which is less than 0.05.

-In reference to paragraph (67): less than two thirds of companies (58.5%) considering all areas for regular review to ensure compliance with security policy, while other companies (17%) do not consider that areas for regular review. This is due to the fact that the mean of responses to this paragraph is 2.54 with a significance level of 0.002 for the sign test, which is less than 0.05.

-In reference to paragraph (68): most of companies (78%) protecting the access to system audit tools to prevent any misuse or compromise, while other companies (4.9%) do not protect the access to system audit tools. This is confirmed since the mean of responses to this paragraph is 3.05 with a significance level of 0.0000 for the sign test, which is less than 0.05.

Testing Hypothesis 10:

There is a significant effect for Compliance with legal requirements on the effectiveness of Information Security Management in Palestinian Information Technology companies.

To test this hypothesis, the researcher used the sign test to check the significance of the Compliance domain.

Table (4. 29): Sign test results of the domain Compliance

Domain	Mean	%	Sign Test
Compliance	2.69	67.25	.0003

The results in Table (4.29) show that the mean of responses on the domain "Compliance" questions is 2.69 and its percentage weight is 67.25%, and the value of sign test is 0.0003 which is less than 0.05. This confirmed that the Compliance with legal requirements in the Palestinian IT companies affecting the effectiveness of Information Security Management in these companies to some extent. This agrees with the study of (Luthy and Forcht, 2006) which stated that organizations worldwide lack explicit references to information management. The authors also added that that awareness of applicable laws and regulations, along with their potential impacts on information management systems, is critical for compliance.

According to the previous results we can accept the hypothesis "**There is a significant effect for Compliance with legal requirements on the effectiveness of Information Security Management in Palestinian Information Technology companies**"

Testing Hypothesis 11:

There are differences denoting a statistical significance between Information Technology companies in Palestine in applying the Information Security Management attributed to the following variables:

-Company age in IT field.

-Type of Operating Systems.

-Staff qualifications.

-Staff experience years

-Company main working field

-Yearly security budget

To test this hypothesis the researcher uses Kruskal-Wallis test for testing the differences between IT companies in applying Information Security Management.

The hypothesis separated into six sub hypotheses and every sub hypothesis tested separately.

Testing Hypothesis 11.1

There are differences denoting a statistical significance between Information Technology Companies in Palestine in applying Information Security Management due to Companies age in IT field.

Table (4. 30): Kruskal-Wallis test for testing the differences between IT companies in applying Information Security Management due to the company age in IT field

#	Variable	Significance	Df	Chi-Square
1	Information Security Management	0.505	3	2.34

The results in the table (4.30) show that the significance of Information Security Management is above 0.05, this denotes that there are no differences between IT companies in applying Information Security Management due to the company age in IT filed.

According to these results; we cannot accept the sub hypothesis "**There are differences denoting a statistical significance between Information Technology Companies in Palestine in applying Information Security Management due to Companies age in IT field**"

Testing Hypothesis 11.2

There are differences denoting a statistical significance between Information Technology Companies in Palestine in applying Information Security Management due to the type of Operating Systems.

Table (4. 31): Kruskal-Wallis test for testing the differences between IT companies in applying Information Security Management due to the type of Operating Systems

#	Variable	Significance	Df	Chi-Square
1	Information Security Management	0.073	2	5.22

The results in the table (4.31) show that the significance of Information Security Management is above 0.05, this denotes that there are no differences between IT companies in applying Information Security Management due to the Operating system.

According to these results; we cannot accept the sub hypothesis "**There are differences denoting a statistical significance between Information Technology Companies in Palestine in applying Information Security Management due to the type of Operating Systems"**

Testing Hypothesis 11.3

There are differences denoting a statistical significance between Information Technology Companies in Palestine in applying Information Security Management due to Staff Qualifications.

Table (4. 32): Kruskal-Wallis test for testing the differences between IT companies in applying Information Security Management due to Staff Qualifications

#	Variable	Significance	Df	Chi-Square
1	Information Security Management	0.188	1	1.73

The results in the table (4.32) show that the significance of Information Security Management is above 0.05, this denotes that there are no differences between IT companies in applying Information Security Management due to Staff Qualifications.

According to these results we cannot accept the sub hypothesis "**There are differences denoting a statistical significance between Information Technology Companies in Palestine in applying Information Security Management due to Staff Qualifications**"

Testing Hypothesis 11.4

There are differences denoting a statistical significance between Information Technology Companies in Palestine in applying Information Security Management due to Staff Experience Years.

Table (4. 33): Kruskal-Wallis test for testing the differences between IT companies in applying Information Security Management due to Staff Experience Years.

#	Variable	Significance	Df	Chi-Square
1	Information Security Management	0.201	1	1.63

The results in the table (4.33) show that the significance of Information Security Management are above 0.05, this denotes that there are no differences between IT companies in applying Information Security Management due to Staff Experience Years.

According to these results we cannot accept the sub hypothesis "**There are differences denoting a statistical significance between Information Technology Companies in Palestine in applying Information Security Management due to Staff Experience Years**"

Testing Hypothesis 11.5

There are differences denoting a statistical significance between Information Technology Companies in Palestine in applying Information Security Management due to the Company Main Working Field.

Table (4. 34): Kruskal-Wallis test for testing the differences between IT companies in applying Information Security Management due to the Company Main Working Field

#	Variable	Significance	Df	Chi-Square
1	Information Security Management	0.868	3	0.723

The results in the table (4.34) show that the significance of Information Security Management is above 0.05, this denotes that there are no differences between IT companies in applying Information Security Management due to the Company Main Working Field.

According to these results we cannot accept the sub hypothesis "**There are differences denoting a statistical significance between Information Technology Companies in Palestine in applying Information Security Management due to the Company Main Working Field**"

Testing Hypothesis 11.6

There are differences denoting a statistical significance between Information Technology Companies in Palestine in applying Information Security Management due to Yearly Security Budget.

Table (4. 35): Kruskal-Wallis test for testing the differences between IT companies in applying Information Security Management due to Yearly Security Budget.

#	Variable	Significance	Df	Chi-Square
1	Information Security Management	0.055	3	7.58

The results in the table (4.35) show that the significance of Information Security Management is above 0.05, this denotes that there are no differences between IT companies in applying Information Security Management due to Yearly Security Budget.

According to these results we cannot accept the sub hypothesis "**There are differences denoting a statistical significance between Information Technology Companies in Palestine in applying Information Security Management due to Yearly Security Budget"**

CHAPTER FIVE: CONCLUSION AND RECOMMENDATIONS

5.1 Conclusion

Following are twelve results founded as the outcome of this thesis:

5.1.1 There is a significant effect for written Information Security Policy on the effectiveness of Information Security Management in Information Technology companies in Palestine, because there is an existing policy which stated the management commitment, and there is a person who is responsible for maintaining the policy according to defined review process which responses to any changes affecting the basis of the original statement.

5.1.2 The Organizational Security in the Palestinian IT companies does not affect the effectiveness of Information Security Management in these companies, the researcher dues that to the lack of reviewing the implementation of security policy in a regular basis. Another reason is the lack of obtaining a specialized information security advice where appropriate

5.1.3 The Asset Classification and Control in the Palestinian IT companies affecting the effectiveness of Information Security Management in these companies because the companies maintaining an inventory with the important assets that associated with information systems, classifying, and labeling the assets in order to assist them handling and protecting these assets.

5.1.4 The Personnel Security in the Palestinian IT companies affecting the effectiveness of Information Security Management in these companies to some extent. The employees did not receive appropriate information security training.

5.1.5 The Physical and Environmental Security in the Palestinian IT companies affecting the effectiveness of Information Security Management in these companies. The companies applying some controls like room locking, following the “on need to know basic” concept,

protecting equipment from power failures, well protecting cables and maintaining the equipment as per suppliers' recommendation.

5.1.6 The Computer and Network Management in the Palestinian IT companies affecting the effectiveness of Information Security Management in these companies. The companies implement many controls to protect their computers and networks; the only lack was in existence of an Incident Management procedure to handle security incidents, and the security policy does not address software licensing issues.

5.1.7 The System Access Control in the Palestinian IT companies affecting the effectiveness of Information Security Management in these companies. Some access controls are applied, and some of such controls are providing each user with a unique identifier and the sensitive systems are provided with isolated computing environment.

5.1.8 The Systems Development and Maintenance in the Palestinian IT companies affecting the effectiveness of Information Security Management in these companies. The data input in the application systems and data output from the applications systems is validated, encryption techniques are used, and there are strict controls in implementing any changes on operational systems.

5.1.9 The Business Continuity Planning in the Palestinian IT companies affecting the effectiveness of Information Security Management in these companies to some extent. This is because of the existence of the process of developing the business continuity plan, some lack was in the testing such plan regularly to ensure that it is up to date and effective.

5.1.10 The Compliance with legal requirements in the Palestinian IT companies affecting the effectiveness of Information Security Management in these companies to some extent. The lack was in existence and well implementing some procedures to ensure compliance with legal restrictions on use of material.

5.1.11 There are no differences denoting a statistical significance between Information Technology Companies in Palestine in applying Information Security Management due to company's history in IT field, operating systems, staff qualifications, staff's years of experience, company main working field, and yearly security budget.

5.2 Recommendations

The following recommendations are directed to IT companies in Palestine, Palestinian government, and to researchers.

1- Information Technology companies are advised to spend a lot of efforts toward the Organizational Security domain.

2- IT companies are advised to enhance their practicing of Personnel Security specially the employees training, finding a formal reporting procedure to report security weaknesses and incidents, and to find a mechanism for quantifying the volume and cost of incidents.

3- IT companies are advised to find an Incident Management procedure to handle security incidents.

4- IT companies are advised to enhance their practicing toward Business Continuity Planning.

5- IT companies are advised to enhance their practicing toward Compliance with legal requirements

6- IT companies are advised to give more concern to the Information Security Management field by following one of the international standards like ISO 17799, or BS 7799.

7-Palestinian Government is advised to prepare Palestinian act that organizing the Information Security field, such act should address the information security crimes and its sanctions.

Future Work

1-Researchers are advised to apply further researchers on IT companies in Palestine by studying the ten domains of Information Security management in more details.

2-Researchers are advised to apply Information Security Management research on governmental ministries.

References

English references

-Bowen, P and others (2006) Information Security Handbook: A Guide for Managers, NIST, Washington.

-Chan, M and Kwok, L (2001) 'Integrating security design into the software development process for e-commerce systems', Information Management & Computer Security 9:3, 112-122.

-Gerber, M (2001) 'Formalizing information security requirements', Information Management & Computer Security 9:1, 32-37.

-Grance, T, Hash, J, and Stevens, M (2004) Security Considerations in the Information System Development Life Cycle, NIST, Washington.

-Grance, T, Kent,K, and Kim, B (2004) Computer Security Incident Handling Guide, NIST, Washington.

-Gritzalis, S, Iliadis, J and Oikonomopoulos, S (2000) 'Distributed component software security issues on deploying a secure electronic marketplace', Information Management & Computer Security, 8:1, 5-13.

-Harold T and Micki K (2004) Information Security Management Handbook, 5th ed., Eds, CRC Press LLC, New York

-Hong, K, Chi, Y, Chao, L, and Tang, J (2003) 'An integrated system theory of information security management', Information Management & Computer Security ,11:5, 243-248.

-Hutchinson, W, Warren, M (2001) 'Attitudes of Australian information system managers against online attackers', Information Management & Computer Security ,9:3, 106-111.

-Irakleous, I and others (2002) 'An experimental comparison of secret-based user authentication technologies', Information Management & Computer Security ,10:3, 100-108.

-Janbandhu, P and Siyal, M (2001) 'Novel biometric digital signature for Internet-based applications', Information Management & Computer Security ,9:5, 205-212.

-Khun, D, and others (2001) Introduction to Public Key Technology and the Federal PKI Infrastructure, NIST, Washington.

-Knapp, K and others (2006) ‘Information security: management’s effect on culture and policy’, Information Management & Computer Security ,14:1, 24-36.
-Krutz, R and Vines, R (2001) The CISSP Prep Guide mastering the ten Domains of Computer Security, John Wiley & Sons, Inc, USA.
-Lankford, W and Johnson, J (2000) ‘EDI via the Internet’, Information Management & Computer Security 8:1, 27-30.
-Lee, J and Lee, Y (2002) ‘A holistic model of computer abuse within organizations’, Information Management & Computer Security 10:2, 57-63.
-Loukis, E (2001) ‘Information systems security in the Greek public sector’, Information Management & Computer Security 9:1, 21-31.
-Luthy, D and Forcht, K (2006) ‘Laws and regulations affecting information management and frameworks for assessing compliance’, Information Management & Computer Security ,14:2, 155-166.
-Maguire, S (2002) ‘Identifying risks during information system development: managing the process’, Information Management & Computer Security ,10:3, 126-134.
-Maiwald, E and Sieglein, W (2002) Security Planning and Disaster Recovery, McGraw-Hill, California
-NIST, (1996), An Introduction to Computer Security The NIST Handbook, NIST, Washington.
-Pastor, M and Dulaney, E (2004) Security+TM Study Guide, SYBEX, Inc, Alameda.
-Phukan, S (2000) ‘Ethics and information technology use: a survey of US based SMEs’, Information Management & Computer Security 8:5, 239-243.
-Purser, S (2004) A Practical Guide to Managing Information Security, Artech House, London.
-Seleznyov, A and Puuronen, S (2003) ‘Using continuous user authentication to detect masqueraders’, Information Management & Computer Security 11:3, 139-145.
-Shim, J, Qureshi, A, and Siegel, J (2000) The International Handbook of Computer Security, Glenlake, Chicago.
-Stanger, J, Lane, P, Crothers, T (2002) CIW Security Professional Study Guide, SYBEX, Inc, San Francisco

-Sunders, M, Lewis, P and Adrian, T (2003) Research Methods for Business Students (3d edn), Prentice Hall, Italy.
-Swanson, M and others (2002), Contingency Planning Guide for Information Technology Systems, NIST, Washington.
-Tilborg, H (2005) Encyclopedia of Cryptography and Security, Eds, Springer, New York
-Tittel, E, Chapple, M and Stewart, J (2003) CISSP Certified Information Systems Security Professional Study Guide, SYBEX, Inc, Alameda.
-Tsoumas, V and Tryfonas, T (2001) 'From risk analysis to effective security management: towards an automated approach', Information Management & Computer Security ,12:1, 91-101.
-Warkentin, M, and Vaughn, R (2005) Enterprise Information Systems Assurance and System Security: Managerial and Technical Issues, IDEA Group Publication, Hershey.
-White, G, and Pearson, S (2001) 'Controlling corporate e-mail, PC use and computer security', Information Management & Computer Security ,9:2, 88-92.
-Wilson, M and Hash, J (2003) Building an Information Technology Security Awareness and Training Program, NIST, Washington
-Ye, N (2001) 'Robust intrusion tolerance in information systems', Information Management & Computer Security 9:1, 38-43.

Arabic references

-أبو علام، رجاء، التحليل الإحصائي للبيانات باستخدام برنامج SPSS، دار النشر للجامعات، القاهرة (2003)

-البلداوي، عبد الحميد، أساليب البحث العلمي والتحليل الاحصائي، الشروق، عمان (2004)

-علام، صلاح الدين، الأساليب الإحصائية الاستدلالية في تحليل بيانات البحوث النفسية والتربوية والاجتماعية (البارامترية واللابارامترية)، دارالفكر العربي، القاهرة (2005)

Internet Websites

-Computer Security Institute, http://www.gocsi.com (Jan 2008)

-Fiedler, A (2003) On the necessity of management of information security, The Standard ISO17799 as international basis http://www.noweco.com/wp_iso17799e.htm (Feb 2008)

-http://www.fbi.gov/cyberinvest/cyberhome.htm

-http://www.iss.net (Jan 2007)

-http://www.sans.org (Jan 2007)

-Weise, J and Martin, C (2001) Developing a Security Policy, Sun BluePrints, http://www.sun.com/blueprints (Jun 2007)

Appendices

Appendix (1)

English Questionnaire

The Islamic University of Gaza
Postgraduate Deanery
Faculty of Commerce
Business Administration

Questionnaire No:_____

Effectiveness of Information Security at the Palestinian IT Companies

Dear Sir/Madam
This questionnaire is aimed to show to which extent the Information Security Management in the Palestinian Information Technology Companies is effective. This will be done by measuring the extent to which the ten domains of information security management are applied.

Through this questionnaire, we will investigate whether the Palestinian Information Technology Companies are using and applying international standards in information security management.

The questionnaire is intended to measure administrative issues, so it's oriented to people working in administrative jobs such as company directors, network administrators, systems administrators, database administrators and technical managers …etc.

I would appreciate your answers to this questionnaire and stress that you will be making a great service to the research process in the Palestinian universities.

Note: The collected data will not be distributed to any third party. It will be used only for the research purposes. No company names will be mentioned in the research documents.

Please put x letter in the box that related to your answer.

Thank you very much for your time.

For further information, please do not hesitate to call me on 0599 601362 or by send an email to alaiddint@yahoo.com.

Researcher
Alaiddin M. Tayeh

Information Security Management

First: General Information:

1- Your Qualification.

☐ Less than diploma ☐ Diploma ☐ Bachelor ☐ High Education

2- Your Specialty.

☐ Computer Engineering ☐ Computer Science ☐ Business Administration ☐ Other (please specify) _____

3- Your experience years in Information Technology field.

☐ Less than two years ☐ Two to five years ☐ Six to ten years ☐ More than ten years

4- Your title in the company (Please select only one option).

☐ Company Director ☐ Systems Administrator ☐ Database Administrator ☐ Network Administrator

☐ Technical Manager ☐ Other (please specify) _____

_____

5- Company age in Information Technology field.

☐ Less than two years ☐ Two to five years ☐ Six to ten years ☐ More than ten years

6- Company main working field (Specialty) (Please select only one option).

☐ Suppliers of equipment in computing and telecommunications ☐ Database Building and manipulations ☐ Geographic Information System (GIS) ☐ Computer Aided Design for Engineers (CAD)

☐ Application software suppliers ☐ Internet service providers ☐ Professional network services suppliers ☐ Professional Technical Training

7- Operating systems used in the company (Please select only one option).

☐ Windows ☐ Linux/Unix ☐ Windows & Linux/Unix ☐ Other (please specify) _____

8- Percentage of Information Security Management Process from the general budget.

☐ Less than 1% ☐ 1% to 3% ☐ 4% to 5% ☐ More than 5%

9-Company Address (City). _____

Second: Research Domains

#	Question	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
	Domain 1: Security Policy					
10.	There exists an Information security policy, which is approved by the management and known by all employees.					
11.	The policy states the management commitment and set out the organizational approach to managing information security.					
12.	The Security policy has an owner, who is responsible for its maintenance and review according to a defined review process.					
13.	The process ensures that a review takes place in response to any changes affecting the basis of the original assessment, example: significant security incidents, new vulnerabilities or changes to organizational or technical infrastructure.					

#	Question	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
	Domain 2: Organizational Security					
14.	There is a cross-functional forum of management representatives from relevant parts of the organization to coordinate the implementation of information security controls.					
15.	Responsibilities for the protection of individual assets and for carrying out specific security processes were clearly defined.					
16.	Specialized information security advice is obtained where appropriate.					
17.	The implementation of security policy is reviewed independently on regular basis. This is to provide assurance that organizational practices properly reflect the policy, and that it is feasible and effective.					

#	Question	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
	Domain 3: Asset Classification and Control					
18.	An inventory or register is maintained with the important assets associated with each information system.(Such register identifies the owner and the location of each asset)					
19.	There is an Information classification scheme or guideline in place; which will assist in determining how the information is to be handled and protected.					
20.	An appropriate set of procedures are defined for information labeling and handling in accordance with the classification scheme adopted by the organization.					

#	Question	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
	Domain 4: Personnel Security					
21.	Security roles and responsibilities as laid in Organization's information security policy are documented in job definitions.					
22.	Employees are asked to sign Confidentiality or non-disclosure agreement as a part of their initial terms and conditions of the employment.					
23.	All employees of the organization receive appropriate Information Security training and regular updates in organizational policies and procedures.					
24.	A formal reporting procedure exists, to report security incidents through appropriate management channels as quickly as possible.					
25.	A formal reporting procedure or guideline exists for users, to report security weakness in, or threats to, systems or services.					
26.	There are mechanisms in place to enable the types, volumes and costs of incidents and malfunctions to be quantified and monitored.					
27.	There is a formal disciplinary process in place for employees who have violated organizational security policies and procedures.					

#	Question	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
	Domain 5: Physical and Environmental Security					
28.	The rooms, which have the Information processing service, are locked or have lockable cabinets or safes.					
29.	The information is only on need to know basis, which means there exists some security controls for third parties or for personnel working in secure area.					
30.	The equipment is protected from power failures by using permanence of power supplies such as multiple feeds, UPS, backup generator etc.					
31.	The power and telecommunications cable carrying data or supporting information services are protected from interception or damage.					
32.	The equipment is maintained as per the supplier's recommended service intervals and specifications.					
33.	Disposal storage device containing sensitive information are physically destroyed or securely over written.					
34.	Automatic computer screen locking facility is enabled. This would lock the screen when the computer is left unattended for a period					

#	Question	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
	Domain 6: Computer and Network Management					
35.	The Security Policy has identified any Operating procedures such as Back-up, Equipment maintenance etc.,					
36.	Audit logs are maintained for any change made to the production programs.					
37.	There is an Incident Management procedure exist to handle security incidents.					
38.	Duties and areas of responsibility are separated in order to reduce opportunities for unauthorized modification or misuse of information or services.					
39.	The capacity demands are monitored and projections of future capacity requirements are made. Example: Monitoring Hard disk space, RAM, CPU on critical servers.					
40.	System acceptance criteria are established for new information systems, upgrades and new versions and suitable tests were carried out prior to acceptance.					
41.	The security policy addresses software licensing issues such as prohibiting usage of unauthorized software.					
42.	Antivirus software is installed on the computers to check and isolate or remove any viruses from computer and media and this software signature is updated on a regular basis to check any latest viruses.					
43.	Back-up of essential business information such as production server, critical network components, configuration backup etc., were taken regularly.					
44.	Faults are reported and well managed. This includes corrective action being taken.					
45.	Effective operational controls such as separate network were established where necessary in order to secure the network.					
46.	There is a policy in place for the acceptable use of electronic mail.					
47.	There are some controls in place to protect the integrity of such information publicly available from any unauthorized access.(such as firewalls)					

#	Question	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
	Domain 7: System Access Control					
48.	The access control policy does address the rules and rights for each user or a group of users.					
49.	There exists a process to review user access rights at regular intervals.					
50.	There are some guidelines in place to guide users in selecting and maintaining secure passwords.					
51.	A unique identifier is provided to every user such as operators, system administrators and all other staff including technical.					

52.	The sensitive systems are provided with isolated computing environment such as running on a dedicated computer, share resources only with trusted application systems.					
53.	An audit logs recording security relevant events are produced and kept for an agreed period to assist in future investigations and access control monitoring.					

#	Question	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
	Domain 8: Systems Development and Maintenance					
54.	The data input to application system is validated to ensure that it is correct and appropriate.					
55.	The data output of application system is validated to ensure that the processing of stored information is correct and appropriate to circumstances.					
56.	Encryption techniques were used to protect the data.					
57.	There are some controls in place for the implementation of software on operational systems. This is to minimize the risk of corruption of operational systems.					
58.	There are strict control procedures in place over implementation of changes to the information system. This is to minimize the corruption of information system.					

#	Question	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
	Domain 9: Business Continuity Planning					
59.	There is a managed process in place for developing and maintaining business continuity throughout the organization.					
60.	The events that could cause interruptions to business process were identified example: equipment failure, flood and fire. A risk assessment was conducted to determine impact of such interruptions and a strategy plan was developed based on the risk assessment results to determine an overall approach to business continuity					
61.	Plans were developed to restore business operations within the required time frame following an interruption or failure to business process.					
62.	There is a single framework of business continuity plan, this framework is maintained to ensure that all plans are consistent and identify priorities for testing and maintenance. Such framework identifies individuals responsible for executing each component of the plan.					
63.	Business continuity plans are tested regularly to ensure that they are up to date and effective.					

#	Question	Strongly Agree	Agree	Neither Agree nor Disagree	Disagree	Strongly Disagree
	Domain 10: Compliance					

64.	All relevant statutory, regulatory and contractual requirements were explicitly defined and documented for each information system. Specific controls and individual responsibilities to meet these requirements were defined and documented.					
65.	There exist and well implemented some procedures to ensure compliance with legal restrictions on use of material in respect of which there may be intellectual property rights (copyright, design rights, trade marks).					
66.	There is a management structure and control in place to protect data and privacy of personal information.					
67.	All areas within the organization are considered for regular review to ensure compliance with security policy, standards and procedures.					
68.	Access to system audit tools such as software or data files are protected to prevent any possible misuse or compromise.					

Appendix (2)

Arabic Questionnaire

الجامعة الإسلامية غزة **رقم الاستبانة: ــــــــ**

عمادة الدراسات العليا

كلية التجارة - إدارة الأعمال

استبانة لتحديد

مدى فعالية إدارة أمن المعلومات في شركات تكنولوجيا المعلومات في فلسطين

الأخ الفاضل... الأخت الفاضلة..

هذه استبانة تهدف إلى تحديد **مدى فعالية إدارة أمن المعلومات في شركات تكنولوجيا المعلومات في فلسطين** وذلك بقياس العشرة مجالات في أمن المعلومات.

من خلال هذه الاستبانة سيتم الوقوف على واقع شركات تكنولوجيا المعلومات في فلسطين والتعرف على مدى تطبيقها للمعايير الدولية في مجال إدارة أمن المعلومات، وبما أن الاستبانة تقيس ذلك الموضوع من ناحية إدارية، فإنها موجهة للأفراد الذين يعملون في وظائف إدارية مثل مدراء الشركات ومدراء الشبكات وقواعد البيانات والدعم الفني وغير ذلك من مواقع إدارية.

وبما أنكم الأكثر معرفة بالوضع القائم في شركاتكم تم التوجه إليكم لتعبئة هذه الاستبانة، ولا تنسوا أن في ذلك مساهمة كبيرة منكم في تطوير عملية البحث العلمي في جامعاتنا الفلسطينية.

ملاحظة: البيانات التي يتم الحصول عليها منكم تستخدم فقط لأغراض البحث العلمي ويراعى فيها السرية التامة، حيث لا يتم التصريح باسم أية شركة عند الحديث عن النتائج.

الرجاء وضع حرف x في المربع المرتبط بإجابتك.

وشكرا جزيلا على وقتك

للاستفسار الرجاء عدم التردد في الاتصال على جوال 0599 601362 أو إرسال رسالة إلى alaiddint@yahoo.com

الباحث

علاء الدين محمود نايه

إدارة أمن المعلومات

أولا: معلومات عامة

1- المؤهل العلمي.

☐ أقل من دبلوم ☐ دبلوم ☐ بكالوريوس ☐ دراسات عليا

2- التخصص.

☐ هندسة حاسوب ☐ علوم كمبيوتر ☐ إدارة أعمال ☐ غير ذلك(الرجاء حدد)

3- عدد سنوات خبرتك في العمل في مجال تكنولوجيا المعلومات.

☐ أقل من سنتين ☐ سنتان – 5 سنوات ☐ 6 – 10 سنوات ☐ أكثر من 10 سنوات

4- المسمى الوظيفي (اختر اجابة واحدة فقط من فضلك).

☐ مدير الشركة ☐ مدير الأنظمة ☐ مدير قواعد البيانات ☐ مدير الشبكة

☐ المدير الفني ☐ غير ذلك (الرجاء حدد):

5- عمر الشركة في مجال تكنولوجيا المعلومات.

☐ أقل من سنتين ☐ سنتان - 5 سنوات ☐ 6 - 10 سنوات ☐ أكثر من 10 سنوات

6- المجال الرئيسي لعمل الشركة(اختر اجابة واحدة فقط من فضلك).

☐ مزود معدات تكنولوجيا واتصال ☐ بناء وتشغيل قواعد بيانات ☐ أنظمة معلومات جغرافية ☐ CAD

☐ مزود تطبيقات برمجية ☐ مزود خدمات إنترنت ☐ مزود خدمات الشبكات ☐ تدريب فني مهني

7- أنظمة التشغيل المستخدمة في الشركة(اختر اجابة واحدة فقط من فضلك).

☐ Windows ☐ Linux/Unix ☐ Windows & Linux/Unix ☐ غير ذلك(الرجاء حدد)

8- نسبة عملية إدارة أمن المعلومات من الموازنة العامة للشركة:

☐ أقل من 1% ☐ 1% إلى 3% ☐ 4% إلى 5% ☐ أكثر من 5%

9- مكـــان عمـــل الـــشركة (المدينة).

ثانيا: مجالات الدراسة

رقم	السؤال	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
	المجال الأول: سياسة الأمن Security Policy					
.10	يوجد في الشركة سياسة لأمن المعلومات معتمدة من قبل الإدارة ويعرفها جميع الموظفين.					
.11	سياسة أمن المعلومات الموجودة تبين مدى التزام الإدارة وطريقة الشركة في إدارة أمن المعلومات.					
.12	هناك شخص محدد ومعروف مسؤول عن سياسة أمن المعلومات ويقوم بمراجعة تلك السياسة وتحديثها من خلال عملية مراجعة محددة مسبقا.					
.13	تأخذ عملية المراجعة بعين الاعتبار الاستجابة لأية تغيرات جديدة (مثال: حوادث أمن مهمة أو مخاطر جديدة أو تغيرات على البنية التحتية الفنية أو التنظيمية).					

رقم	السؤال	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
	المجال الثاني: الأمن التنظيمي Organizational Security					
.14	يوجد في الشركة فريق (مكون من أفراد ممثلين لجميع الأقسام) مسؤول عن إدارة أمن المعلومات.					
.15	مسؤوليات حماية ممتلكات الأفراد وتنفيذ عمليات أمن محددة تم تعريفها بشكل واضح.					
.16	تقوم الشركة بالاستعانة بخبراء للحصول على استشارات في أمن المعلومات.					
.17	يتم مراجعة تنفيذ سياسة الأمن من قبل جهة مستقلة وبشكل دوري للتأكد أن الشركة تمارس السياسة بشكل جيد، وأن هذه السياسة ذات جدوى وفعالية.					

رقم	السؤال	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
	المجال الثالث: تصنيف الأصول(الممتلكات) وضبطها Asset classification and control					
.18	تستخدم الشركة سجلا لحفظ بيانات الأصول ذات العلاقة بكل نظام من أنظمة المعلومات.(يبين السجل مستخدم ذلك الأصل ومكان وجوده).					
.19	يوجد جدول أو دليل تصنيف للمعلومات من شأنه أن يساعد في تحديد الكيفية التي يتم التعامل بها مع المعلومات وحمايتها.					
.20	يوجد مجموعة من الإجراءات المناسبة لعنونة المعلومات والتعامل معها طبقا لجدول التصنيف.					

رقم	السؤال	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
	المجال الرابع: الأفراد وأمن المعلومات Personnel Security					
.21	تحتوي وثيقة الوصف الوظيفي للموظف على مسؤولياته ومهامه تجاه أمن المعلومات في الشركة.					
.22	يتم الطلب من الموظفين التوقيع على تعهد بعدم الإفصاح عن معلومات الشركة كجزء من شروط توظيفهم.					
.23	يتلقى جميع الموظفين تدريبا مناسبا خاصا بأمن المعلومات، ويتم إطلاعهم على آخر التحديثات على سياسات وإجراءات أمن المعلومات في الشركة.					
.24	تتبع الشركة إجراءا رسميا لرفع التقارير بحوادث الأمن في الشركة من خلال القنوات الإدارية المناسبة وبالسرعة الممكنة.					
.25	يوجد إجراءا رسميا يتبعه المستخدمون لرفع التقارير بمواطن الضعف والمخاطر الأمنية في الأنظمة والخدمات.					
.26	يوجد آليات مطبقة تمكن من متابعة وتقدير أنواع وأحجام وتكاليف حوادث الأمن والتلف الذي تحدثه.					
.27	يتم تطبيق إجراءات تأديبية رسمية على الموظفين الذين ينتهكون إجراءات وسياسات أمن المعلومات في الشركة.					

رقم	السؤال	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
	المجال الخامس: الأمن المكاني Physical and Environmental Security					
.28	الغرف التي تحتوي على الأجهزة والمعلومات تكون مغلقة أو بها خزانات آمنة يمكن إغلاقها.					
.29	المعلومات متاحة فقط على أساس الحاجة لها، بمعنى أنه يوجد ضوابط تحكم دخول الأفراد الخارجيين والأفراد الذين يعملون في مناطق آمنة.					
.30	الأجهزة محمية من انقطاع الكهرباء، بمعنى أنه يوجد في الشركة مولد كهرباء احتياطي، UPS ، أكثر من خط كهرباء.					
.31	كوابل الكهرباء والاتصالات التي تحمل البيانات أو تدعم خدمات المعلومات محمية من العبث بها أو إتلافها.					
.32	يتم عمل صيانة للمعدات بناءا على توصيات ونصائح المزود من حيث المواصفات والمواعيد.					
.33	يتم التخلص جيدا من أجهزة حفظ البيانات التي تحتوي على بيانات حساسة وتتعطل أو تصبح لا لزوم لها وذلك بالإتلاف أو الكتابة فوقها.					
.34	يتم تأمين شاشة الحاسوب بشكل يدوي أو آلي عند عدم استخدامها لفترة ما.					

رقم	السؤال	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
	المجال السادس: إدارة الشبكة والحواسيب Computer and Network Management					

.35	سياسة الأمن تحدد إجراءات التشغيل مثل النسخ الاحتياطي وصيانة الأجهزة وغير ذلك.					
.36	يتم استخدام سجلات تدقيق لأية تغيرات تتم على الأنظمة العاملة في الشركة.					
.37	هناك إجراء إدارة أحداث موجود للتعامل مع أحداث أمن المعلومات.					
.38	المهام ونطاق المسؤوليات عن الأجهزة والأنظمة منفصلة وذلك من أجل تقليل فرص إجراء تغييرات غير مسموح بها أو منعا لإساءة الاستخدام.					
.39	يتم متابعة احتياجات الأجهزة، وعمل توقع لمتطلباتها المستقبلية مثل (H.D, CPU, RAM).					
.40	هناك معايير لقبول أية أنظمة جديدة أو أية تعديلات أو نسخ جديدة، ويتم إجراء اختبارات عليها قبل القبول بها.					
.41	تبين سياسة الأمن أمورا ذات علاقة بترخيص البرامج، مثل منع استخدام برامج غير مرخصة.					
.42	يتم استخدام برامج لمراقبة مكافحة وإزالة الفيروسات ويتم تحديث هذه البرامج باستمرار.					
.43	يتم عمل نسخ احتياطي للمعلومات المهمة بشكل دوري.					
.44	يتم تسجيل وتوثيق الأخطاء التي تحدث في تقارير توضحها و توضح الإجراءات التي تم اتخاذها لتصحيحها.					
.45	يتم استخدام ضوابط تشغيلية مثل عزل الشبكة عند الضرورة وذلك لحماية الشبكة من المخاطر.					
.46	يوجد سياسة خاصة بالاستخدام المقبول للبريد الإلكتروني.					
.47	يتم استخدام ضوابط لحماية سلامة المعلومات المتاحة للعامة من الوصول الغير مسموح به، مثل استخدام جدران نارية واكتشاف أية اقتحامات.					

رقم	السؤال	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
	المجال السابع: ضبط الوصول للأنظمة System Access Control					
.48	تبين سياسة ضبط الوصول القواعد والصلاحيات لكل مستخدم أو مجموعة من المستخدمين.					
.49	يوجد عملية دورية لمراجعة صلاحيات المستخدمين في الوصول للأنظمة.					
.50	يوجد توجيهات مطبقة لإرشاد المستخدمين في اختيار كلمات المرور والمحافظة عليها.					
.51	يوجد حساب (اسم مستخدم/ وكلمة مرور) خاص لكل مستخدم مثل الفنيون ومديرو الأنظمة والمشغلون، بمعنى أنه لا يتم استخدام حسابات عامة يستخدمها أكثر من شخص.					
.52	يتم عزل الأنظمة الحساسة في بيئة عمل منفصلة، مثلا أن تكون على جهاز مستقل وتتشارك المصادر فقط مع الأنظمة الموثوقة.					
.53	يتم استخدام سجلات متابعة لحفظ أحداث ذات علاقة بالأمن، ويتم الاحتفاظ بها لفترة زمنية متعارف عليها، وذلك للمساعدة في أية تحقيقات مستقبلية.					

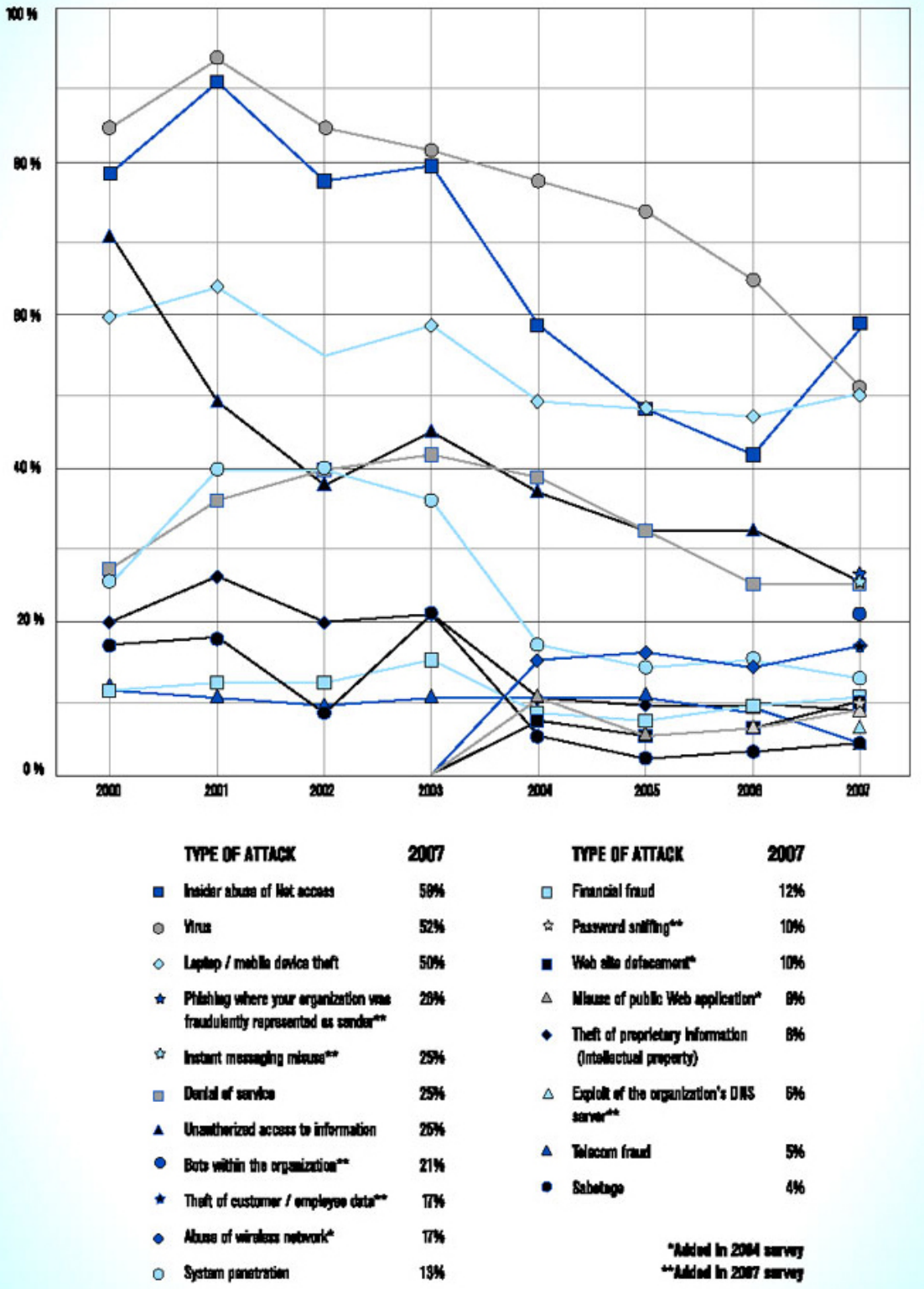
رقم	السؤال	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
	المجال الثامن: تطوير وصيانة الأنظمة Systems development and maintenance					
.54	يتم التحقق من صحة البيانات المدخلة للأنظمة للتأكد أنها صحيحة ومناسبة.					
.55	يتم التحقق من المخرجات الناتجة من الأنظمة للتأكد أن معالجة المعلومات المخزنة تمت بشكل صحيح.					
.56	يتم استخدام آليات تشفير لحماية البيانات.					
.57	يوجد ضوابط مطبقة على تنفيذ البرامج على أنظمة التشغيل، وذلك بهدف تقليل مخاطر تعرض أنظمة التشغيل للتلف.					
.58	يوجد إجراءات ضبط صارمة مطبقة على تنفيذ أية تغييرات على أنظمة المعلومات، وذلك لحمايتها من العطل.					

رقم	السؤال	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
	المجال التاسع: تخطيط استمرارية العمل Business Continuity Planning					
.59	يتم في الشركة تطوير واستخدام خطة لاستمرارية العمل (هذا قد يتطلب خطة واسعة على مستوى الشركة، اختبار وتعديل دوري على الخطة، تشكيل وتوثيق استراتيجية لاستمرارية العمل).					
.60	تم تحديد وتعريف الأحداث التي قد تؤدي إلى توقف العمل، وتم عمل تقدير مخاطر لتحديد أثر تلك الأحداث على العمل، وبناء عليه تم عمل خطة إستراتيجية لتحديد الأسلوب المتبع لاستمرارية العمل.					
.61	يوجد خطة لإعادة الأعمال إلى طبيعتها ضمن الإطار الزمني المطلوب بعد حدوث إخفاق أو انقطاع في أداء العمل.					
.62	يوجد إطار عمل موحد لخطة استمرارية العمل، ويتم استخدامه للتأكد من أن جميع الخطط متوافقة ولتحديد الأولويات في الاختبار والاستخدام، ويحدد ذلك الإطار الأفراد المسؤولين عن تنفيذ كل جزء من الخطة.					
.63	يتم اختبار خطط استمرارية العمل بشكل دوري للتأكد من أنها محدثة وفعالة.					

رقم	السؤال	موافق بشدة	موافق	محايد	غير موافق	غير موافق بشدة
	المجال العاشر: الامتثال للمتطلبات القانونية Compliance					
.64	تم تحديد وتوثيق المتطلبات القانونية والتنظيمية والتعاقدية ذات العلاقة بكل نظام معلومات، وتم تحديد وتوثيق الضوابط والمسؤوليات الفردية لتلبية تلك المتطلبات.					
.65	يوجد إجراءات للتأكد من الامتثال للقيود القانونية في استخدام المواد التي قد يكون لها حقوق ملكية فكرية، مثل حقوق الطبع والتصميم والعلامات التجارية.					
.66	يوجد هيكل إداري وضوابط لحماية البيانات وخصوصية معلومات الأفراد.					
.67	يتم عمل مراجعة دورية لجميع أجزاء الشركة للتأكد من الامتثال لسياسة الأمن والإجراءات والمعايير.					
.68	يمكن اعتبار أن الوصول لأدوات مراقبة ومتابعة الأنظمة مثل البرامج وملفات البيانات محمية وذلك لمنع إساءة استخدامها.					

Appendix (3)

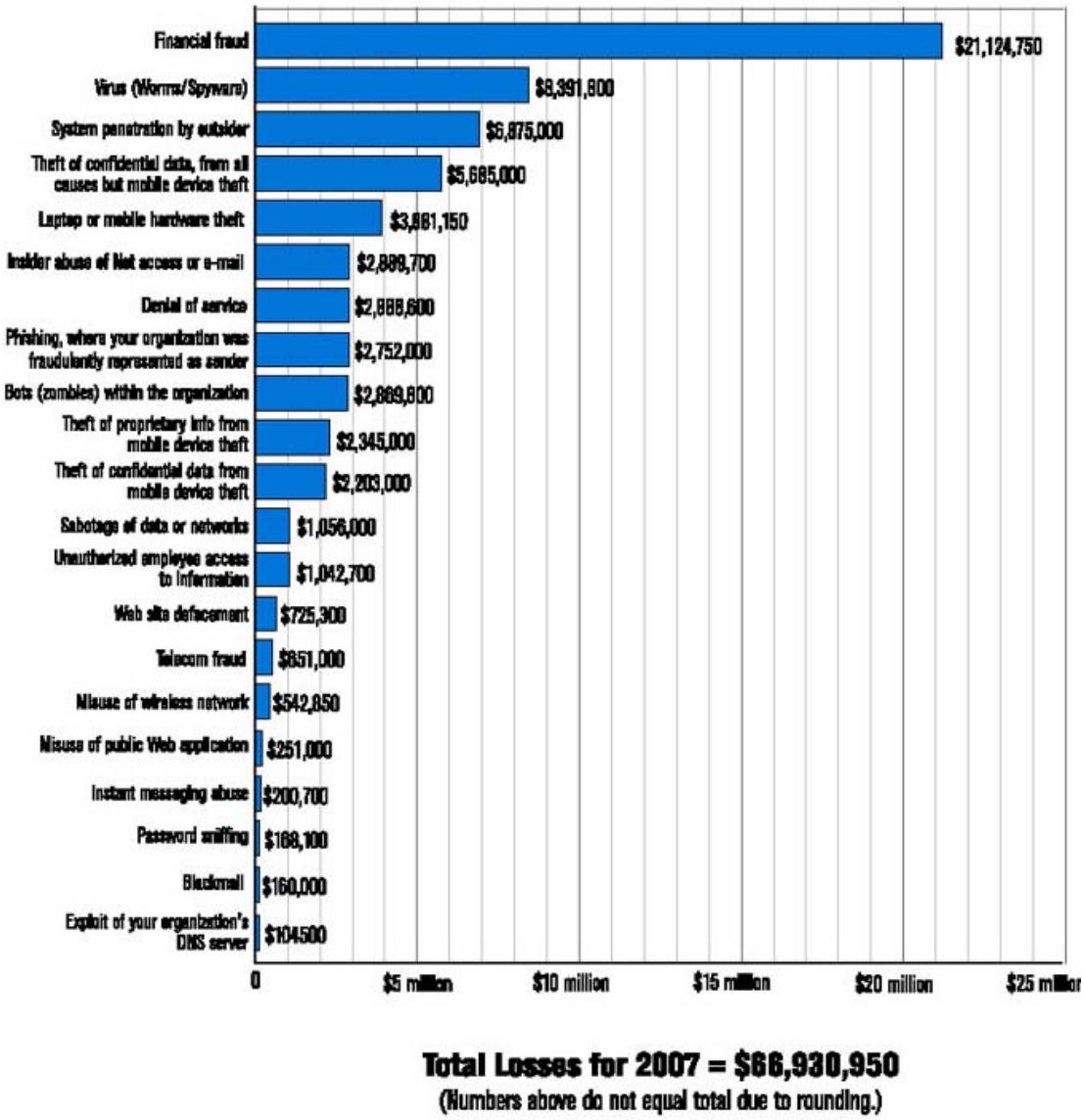
Types of attacks and misuses detected in the year 2007.



Source: (2007 CCSS) http://www.gocsi.com, (Jan 2008)

Appendix (4)

Dollar Amount Losses by Type of Attack

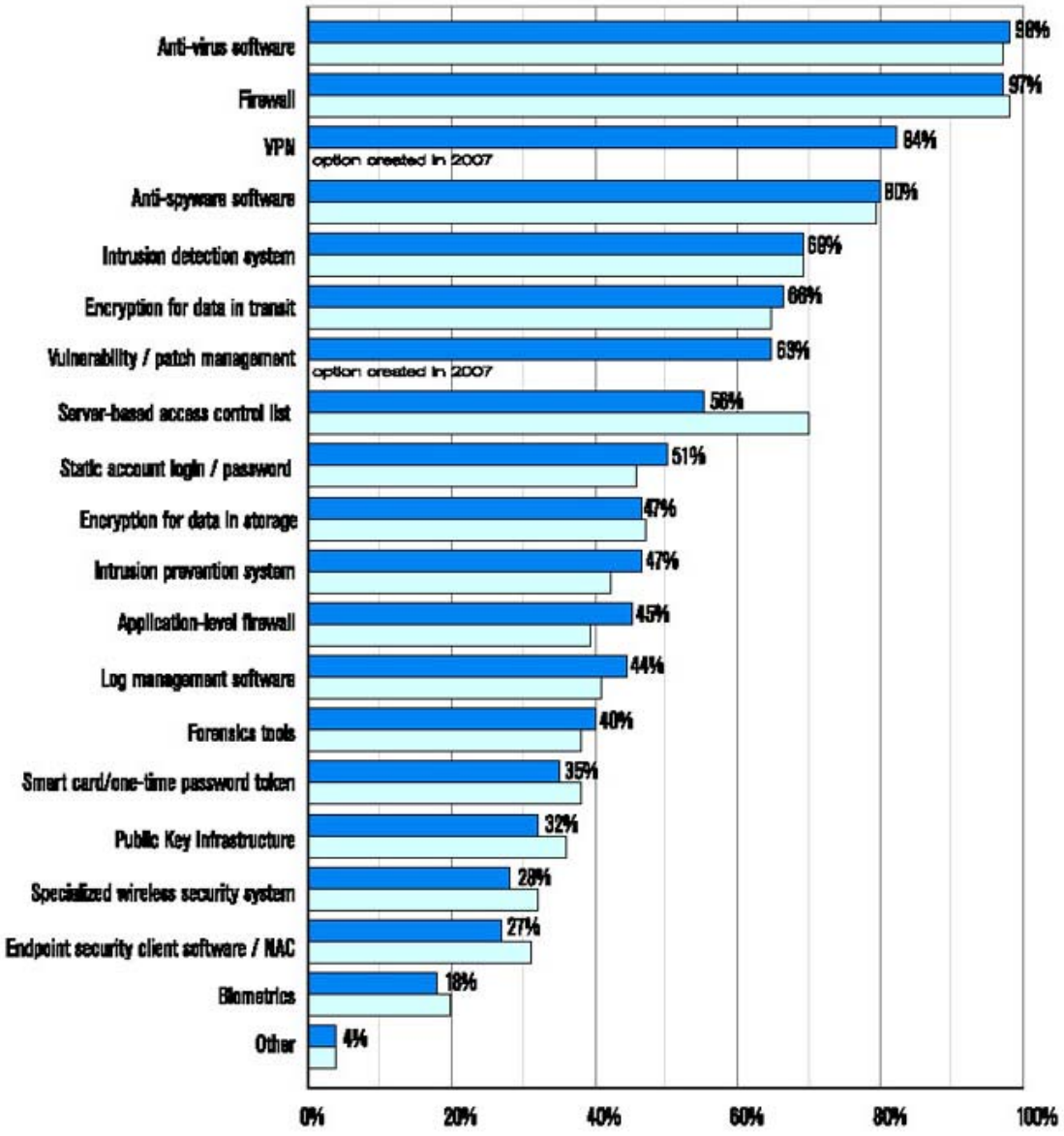


Total Losses for 2007 = $66,930,950
(Numbers above do not equal total due to rounding.)

Source: (2007 CCSS) http://www.gocsi.com, (Jan 2008)

Appendix (5)

Security Technologies Used



Source: (2007 CCSS) http://www.gocsi.com, (Jan 2008)

Appendix (6)

American and European Computer Security Laws, Regulations, and Directives.

1970 U.S. Fair Credit Reporting Act.

1970 U.S. Racketeer Influenced and Corrupt Organization Act (RICO).

1973 U.S. Code of Fair Information Practices.

1974 U.S. Privacy Act.

1980 Organization for Economic Cooperation and Development (OECD) Guidelines.

1984 U.S. Medical Computer Crime Act.

1984 (Strengthened in 1986 and 1994) First U.S. Federal Computer Crime Law Passed.

1986 (Amended in 1996) U.S. Computer Fraud and Abuse Act.

1986 U.S. Electronic Communications Privacy Act.

1987 U.S. Computer Security Act.

1990 United Kingdom Computer Misuse Act.

1991 U.S. Federal Sentencing Guidelines.

1992 OECD Guidelines to Serve as a Total Security Framework.

1995 Council Directive (Law) on Data Protection for the European Union (EU).

1996 U.S. Economic and Protection of Proprietary Information Act.

1996 U.S. Kennedy-Kassenbaum Health Insurance and Portability Accountability Act (HIPAA) (with the additional requirements added in December of 2000).

1996 U.S. National Information Infrastructure Protection Act.

Generally Accepted Systems Security Principles (GASSP).

Source: (Krutz and Vines, 2001, P: 289-290).