UNIVERSITY OF BAHRAIN

College of Information Technology

جامعة البحرين
المكتبة
LIBRARY
University of Bahrain

Improving the Security of Storage Systems Using Cloud Computing

A Thesis Submitted in Partial Fulfillment of the Requirements for the Master Degree in IT

Submitted by

Hanin Mohammed Abdullah

University number: 20114653

Supervised by

Wasan Shaker Awad

(Associate professor)

University of Bahrain

Kingdom of Bahrain

December, 2014

جامعة البحرين
LIBRARY
University of Bahrain

DECLARATION

I declare that this work is the result of my own investigation and that it has not already been accepted in substance for any degree, nor is it currently submitted for any degree.

Signed: ---------- Date: 18-12-2014

Hanin Mohammed Abdullah (Candidate)

The Thesis defense committee considers the Thesis titled:

IMPROVING THE SECURITY OF STORAGE SYSTEMS USING CLOUD COMPUTING

Submitted by Hanin Mohammed Abdullah to the College of Information Technology is satisfactory and acceptable for the Master of Science in Information Technology.

Thesis Defense Committee:

Dr. Wasan Shaker Awad
(Supervisor)
Department of Information Systems
University of Bahrain

Dr. Abderezak Touzene
(Member)
Sultan Qaboos University, Oman

Dr. Ahmad Mashhour
(Member)
Department of Information Systems
University of Bahrain

Abstract

Cyber security is an evolving critical and important topic that has affected IT systems, organizations and technology trends. The importance of information that resides on storage systems exceeds all other IT systems in an organization. This importance makes a breach in the confidentiality, integrity or availability of storage systems unacceptable.

In this thesis, storage systems and cyber security are introduced. An assessment plan for evaluating cyber security of local storage systems in organizations is proposed. This assessment plan is based on research and literature available in the fields of risk and security assessments, cyber security and storage technologies. The assessment proposed has been implemented on two prestigious and important organizations in the Kingdom of Bahrain. These organizations and the outcomes of the cyber security risk assessment of their storage systems are believed to reflect the cyber security status of local storage systems in majority of organizations. Storage systems of the assessed organizations found to have cyber security risks of different scales. This conclusion gives certainty to the fact that organizations are not capable of following the cyber security evolution and secure their storage systems from cyber security vulnerabilities and breaches. Utilizing cloud computing for storage systems is introduced in the thesis. The benefits of migrating storage services to the cloud are discussed. Cyber security effects of such a transition for storage systems are presented in the thesis thoroughly. This thorough study includes the effects of this transition to the available cyber security issues. In addition, breaches that are introduced because of the transition due to the nature of cloud computing services are also presented.

In this thesis, a migration of storage services to cloud is found to solve most of the existing cyber security issues in local storage systems. This is found to be a result of different features of cloud providers such as staff dedication and specialization. On the other hand, a number of cyber security breaches enablers found to be a direct result of a migration such as public networks exposure and multitenant shared infrastructure.

This work is dedicated to my small family. Husband, Mom, Dad, Brothers and the coming Baby, without your love and support none of this work or any achievement in my life would have been possible.

Acknowledgment

Completing my masters' courses and thesis was truly a journey of knowledge and experience. I have loved research, storage systems, cyber security, cloud computing and University of Bahrain. I am indebted to a lot of people around me whom without the aid and support of I wouldn't be able to complete the journey.

First of all I am deeply grateful to my major professor Dr. Wasan Shaker, not only for her guidance through the thesis, also not only for her review, revise and re-revise of my thesis, but also because she has inspired me in the courses I had with her. I am also grateful to Dr. Nabil Hewahi for his guidance and support.

I would like to thank Dr. Hessa Al-Junaid for her guidance in technical writing of thesis. I would like to express my sincere gratitude to Dr. Hesham Al-Ummal, Dean of IT Faculty, for continuous support throughout the journey.

I would like to thank my thesis committee members for their valuable time spent on reviewing this thesis and for their suggestions and advices. Before appreciating people outside University of Bahrain, I am very grateful to the following professors who had been very generous in transferring the knowledge and ideas they have in their courses, Dr. Salman Khan, Dr. Ali Khan, Dr. Yousif Harrath, Dr. Ahmad Zaki and Dr. Ahmed Mashhour. Appreciation also is a must for Dr. Hesham Al-Rawi.

Last but not least, my sincere thanks to my parents for their unconditional support. I would like to thank my dad, Dr. Mohammed Abdulla, for his continues and never ending support and encouragement. I would like also to thank my mother and brothers for their patience and understanding in all of the hard and difficult times. I sincerely thank my

husband, for his sacrifice during our first years of marriage. I also thank my Husband family for their support and prayers as well.

I thank all of my friends and people around me for everything they have given me and surrounded me with their love and prayers.

Table of Content

Subject	Page No
Abstract	II
Acknowledgment	IV
Table of Contents	VI
List of Tables	XII
List of Figures	XIII
List of Appendix	XV
Abbreviations and Definitions	XVII
Chapter One Introduction	
1.1 Thesis Motivations and Problem Statement	2
1.2 Thesis Objective	3
1.3 Scope of the thesis	4
1.4 Highlights of Thesis Contribution	5
1.5 Thesis Outline	5
Chapter Two Theoretical Background and Literature Review	
2.1 Definition of Storage Systems	9
2.2 History of Storage Systems	10
2.3 Storage Systems Basics	13

2.3.1 Major Computer Storage Categories	13
2.3.2 File System	13
2.3.3 Memory Access Methodologies	14
2.3.4 Block and File level storage access	14
2.4 Storage Systems Types	15
2.4.1 Direct-Attached Storage DAS	15
2.4.2 Network-Attached Storage NAS	16
2.4.3 SAN	18
2.5 Cyber security Framework	19
2.5.1 Confidentiality	21
2.5.2 Integrity	21
2.5.3 Availability	21
2.5.4 Other Properties	22
2.6 Risk Triad	23
2.6.1 Assets	23
2.6.2 Threats	24
2.6.3 Vulnerabilities	28
2.7 Storage Security Domains	29
2.7.1 Securing the Application Access Domain	30
2.7.2 Securing the Management Access Domain	34
2.7.3 Securing Backup, Replication, and Archive	35
2.8 Literature Review	37

Chapter Three Cloud Computing	
3.1 Definition of Cloud Computing	41
3.2 Cloud Types and Models	42
3.2.1 Deployment Models	42
3.2.2 Service Models	43
3.3 Cloud Computing Characteristics	46
3.3.1 Advantages	46
3.3.2 Disadvantages	49
3.4 Cloud Architecture and Infrastructure	51
3.5 Challenges and Future of Cloud Computing	52
Chapter Four Storage System Cyber Security Assessment Case Study	
4.1 Assessment Plan for the Local Storage System	55
4.1.1 Quantitative and Qualitative Assessment	55
4.1.2 Targeted Domains of the Assessment	56
4.1.3 Risk Matrix	56
4.1.4 Local Storage System Assessment	58
4.2 Pre-Assessment Questionnaire for Storage Systems Custodians	61
4.3 Storage Security Domains, Criterions, and Weighing Questionnaire for Cyber security Systems Custodians	61
4.3.1 Application Access Security Domain	61

4.3.2 Management Access Security Domain	61
4.3.3 Backup, Replication and Archive Security Domain	61
4.4 Supporting Questionnaire for discussion and conclusions	62
4.5 Assessment of Local Storage Systems of Organization "Alpha"	62
4.5.1 Assessment Results	63
4.5.2 Discussion and Conclusions	68
4.6 Assessment of Local Storage Systems of Organization "Beta"	72
4.7 Techniques for Improving Security of Local Storage Systems	77
Chapter Five Cyber Security of Cloud Storage Services and Proposed Solution	
5.1 Legacy Storage Systems and Cyber security Issues	86
5.2 Cloud Computing for Storage Services	87
5.3 Migrating Storage to Cloud	88
5.4 Cyber security of Storage on Cloud	89
5.4.1 Benefits for Inherited Issues	90
5.4.2 Introduced Issues	92
5.5 Storage Enhanced Security Recommendations	93
5.5.1 Organizational Steps for optimum security of storage	94

systems	
5.5.2 Cloud Migration Proposal	96
5.5.3 Mitigations against introduced cyber security threats of cloud computing	101
Chapter Six Conclusion and Future Work	
6.1 Thesis Conclusion	104
6.2 Future work	105
References	106
Appendix A Local Storage Systems Assessment Questionnaire	
1. Pre-Assessment Questionnaire for Storage Systems Custodians	
2.Questionnaire for Information Security Systems Custodians	
3. Supporting Questionnaire for discussion and conclusions	
Appendix B Alpha Case Study, Information Security of Local Storage Systems	
1. Pre-Assessment Questionnaire for Storage Systems Custodians	
2.Questionnaire for Information Security Systems Custodians	
3. Supporting Questionnaire for discussion and conclusions	
4. Assessment Results Table	
Appendix C Beta Case Study, Information Security of Local Storage	

Systems	
1. Pre-Assessment Questionnaire for Storage Systems Custodians	
2. Questionnaire for Information Security Systems Custodians	
3. Supporting Questionnaire for discussion and conclusions	
4. Assessment Results Table	
(تحسين امن اجهزة خزن البيانات باستخدام الحوسبة ملخص الرسالة باللغة العربية السحابية)	

List of Tables

NO.	Subject	Page No.
1	Table (1) Assessment Results of Organization "Alpha" Storage Systems Cyber security	64
2	Table (2) Risk Matrix Results of "Alpha"	69
3	Table (3) Assessment Results of Organization "Beta" Storage Systems Cyber security	73
4	Table (4) Risk Matrix results of "Beta"	75

List of Figures

No.	Figure	Page No.
1	Figure (1) Evolution of data storage systems -1	11
2	Figure (2) Evolution of data storage systems -2	11
3	Figure (3) A Sample Architecture that utilizes DAS Storage in a small network	16
4	Figure (4)A Sample Architecture that utilizes NAS Storage in a small network	17
5	Figure (5) A Sample Architecture that utilizes SAN Storage in a small network	19
6	Figure (6) Cyber security Triangle CIA	20
7	Figure (7) Security Threats Classification	25
8	Figure (8) Storage System Security Domains	30
9	Figure (9) Security threats in Application access domain	31
10	Figure (10) Security threats in Management access domain	34
11	Figure (11) Security threats in the Backup domain	37
12	Figure (12) Cloud Service Models	45
13	Figure (13) Cloud Definition Components	51
14	Figure (14) Cloud Virtualized Architecture	52
15	Figure (15) Equal distribution risk matrix based on Australian standard	57
16	Figure (16) Heat Diagram of Canadian public safety risk matrix	57
17	Figure (17) 3 by 3 Risk matrix utilized in this thesis	58
18	Figure (18) Overall sequential processes of the Security Risk Assessment	60
19	Figure (19) Criterion Questions Results for "Alpha"	68

20	Figure (20) Risk rating percentages for “Alpha"	69
21	Figure (21) Criterion Questions Results of "Beta"	74
22	Figure (22) Risk Rating Percentages for "Beta"	75
23	Figure (23) Overall Questions status of the two organizations Assessed	77

List of Appendix

No.	Appendix
(1)	Appendix A. Local Storage Systems Assessment Questionnaire
(2)	Appendix B. Alpha Case Study, Information Security of Local Storage Systems
(3)	Appendix C. Beta Case Study, Information Security of Local Storage Systems

Abbreviations and Definitions

BCM	Business continuity Management
BD	Blu-ray Disk
BD-R	Blu-ray Disk Recordable
BD-RE	Blu-ray Disk Rewritable
CAM	Content-Addressable Memory
CAPEX	Capital Expenditure
CCNA	Cisco Certified Network Associate
CD	Compact Disk
CD-R	Compact Disk Recordable
CD-RW	Compact Disk Rewritable
CIA	Confidentiality, Integrity and Availability
CIO	Central Informatics Organization
CPU	Central Processing Unit
DAS	Direct Attached Storage
DNS	Domain Name System
DoS	Denial of Service
DRP	Disaster Recovery Plan
DVD	Digital Video Disk
DVD-R	Digital Video Disk Recordable
DVD-RW	Digital Video Disk Rewritable
EEPROM	Electrically Erasable Programmable Memory
ETSI	European Telecommunication Standards Institute
FAT	File Allocation Table
FC SAN	Fiber Optic SAN

FC-SP	Fiber Channel Secure Protocol
HBA	Host Bus Adapter
HDD	Hard Disk Drive
HFS+	Hierarchical File System Plus
IaaS	Infrastructure-as-a-Service
I/O	Input / Output
IBM	International Business Machines Corporation
IDP	Intrusion Detection and Prevention Systems
IP SAN	Internet Protocol SAN
IP	Internet Protocol
IRM	Information rights management
iSCSI	Internet Small Computer System Interface
ISO9660	File system that is published by ISO for optical disk media
IT	Information Technology
ITU	International Telecommunication Union
LAN	Local Area Network
MCSA	Microsoft Certified Solutions Associate
NA	Not Applicable
NAS	Network Attached Storage
NIST	National Institute of Standards and Technology
NTFS	New Technology File System
OPEX	Operating Expenditure
OS	Operating System
PaaS	Platform-as-a-Service
PM	Preventive Maintenance

RAID	Redundant Array of Inexpensive Disks
RAM	Random Access Memory
RBAC	Role Based Access Control
ReFS	Resilient File System
ROM	Read-Only Memory
SaaS	Software-as-a-Service
SAN	Storage Area Network
SBE	Symantec backup Exec
SCM	Storage Class Memory
SCSI	Small Computer System Interface
SD	Secure Digital Card
SIEM	Security Information and Event Manager
SMR	Shingled Magnetic Recording
SNMP	Simple Network Management Protocol
SSD	Solid State Drives
SSP	Storage Service Providers
Syslog	Standard for computer message logging
TCP	Transmission Control Protocol
UDF	Universal Disk Format
UFS	UNIX File System
VMFS	Virtual Machine File System
WAN	Wide Area Network
WORM	Write Once Read Many

Chapter 1: Introduction

1.1 Thesis Motivations and Problem Statement

1.2 Thesis Objective

1.3 Scope of the thesis

1.4 Thesis Outline

1.5 Highlights of Thesis Contribution

Chapter 1: Introduction

In this chapter, the facts and situation that has led to the importance of the thesis area of research and topic are presented. In addition, the boundaries of this thesis and how it differs from the research available is discussed followed by an overview of the structure of the thesis. This chapter is concluded by presenting a research background and literature review of the topic of this thesis.

1.1 Thesis Motivations and Problem Statement

In the old days, organizations and enterprises have had almost always a file server that is located in a corner without being used because employees were relying on their local disk drives. Nowadays, everything has changed and storage systems are of high importance and of different applications and information (Ateeq, 2012).

The decision of choosing a particular storage system over another for a specific application and the way the system is managed after commissioning is not straight forward and depends on several factors one of which is the cyber security which is the area of research and concern in this thesis.

Cyber Security of Systems is becoming a major issue worldwide and it is being discussed on the highest level of decision makers. Having this said, the security of important systems which affects the performance of organizations should be assessed and improved (Ateeq, 2012). One of these systems is the storage system which has currently many breaches and vulnerabilities in most of the organizations. Some of those vulnerabilities are the lack of access control, weak password policies and ineffective firewall rules.

Cloud computing as an evolving topic is being addressed as an alternative of local systems for organizations. Having cyber security as a

hot topic which cannot be ignored in any study or Information Technology (IT) consideration, migrating storage services to cloud should be assessed as well. In fact, some IT professionals believes in cloud as an enhancement to the cyber security paradigm and some are on the opposite side of the table believing that cloud deteriorate cyber security models (Ateeq, 2012).

This study is motivated by the mentioned factors to assess the traditional storage servers from security point of view, and finds a solution to the threats found. In addition, using cloud storage services instead of the traditional storage server is studied from cyber security point of view as well. A model is proposed in conclusion for organizations to consider.

1.2 Thesis Objective

The main objective of this thesis is to answer the following questions regarding the cyber security of the current storage system and cloud storage services:

- What are the current security challenges in the current locally hosted storage servers?
- Will migrating to cloud services solve the current challenges with current system?
- What are the security threats which are attached to the transition from locally hosted to cloud services?
- What are the security techniques which can mitigate these threats?
- How the security techniques can be integrated in a one secure system design for cloud computing services?

Those are example questions among several others questioning the security of cloud computing services.

1.3 Scope of the thesis

This thesis aims to study the security of file storage server of an organization. Different kinds of security threats and a number of security techniques used to protect information will be examined. Then, a cloud-based system will be proposed to improve the security of storage systems.

The proposed solution is a transition from the current storage server located on the local network to the storage services available on the cloud. These services provided by different vendors specifically tailored to the needs of enterprises. The transition will introduce new security risks and challenges which will be also analyzed in this study.

Cyber security has recently become part of the warfare between countries. It has currently an importance for individuals and enterprises. Also, it gains more importance when it touches the security of important systems such as the storage server which is being discussed and assessed in this thesis.

The storage server is a major asset that saves all of the important files of the organization especially for an education prestigious organization. Cloud computing is an upcoming paradigm that offers tremendous advantages in economical aspects, such as reduced time to market, flexible computing capabilities, and limitless computing power (Gupta & Kaur, 2013).

Having said all of that assessing the security of the storage servers and hardening it with proposed solution in addition to taking into consideration the transition to the cloud is a very important thesis. Thus, this study will help to improve the traditional storage systems in term of security by proposing a secured cloud based system.

1.4 Highlights of Thesis Contribution

The following are the points that are important to highlight as a major contribution of the research done in this thesis

- Risk assessment model for cyber security of local storage systems has been proposed.
- The model is based on the idea of cyber security domains and criterion.
- The proposed model has been implemented on two organizations by interviewing organizations' specialists and acquiring answers to the assessment model questionnaire.
- Security techniques required to mitigate the identified risks have been discussed.
- In the thesis, utilization cloud for storage services is assessed.
- The cyber security aspect of such utilization is thoroughly studied.
- The thesis is concluded with a proposal for secure utilization of cloud computing for organizational storage requirements.
- The proposal takes into consideration many aspects of cloud services contracts and technological requirements.

1.5 Thesis Outline

It is worth to mention that very well known about specialists in Computer Science and Engineering Acronyms and Abbreviations are very common in the syntax of their literature. To avoid any confusion Acronyms and Abbreviations are written in its full format wherever mentioned for the first time in this thesis. In addition, all Acronyms and Abbreviations used in this thesis are listed here along with its full format.

After preliminary pages, chapter one starts with presenting facts that have motivated the research done in this thesis. After that the scope of the thesis followed by this outline is presented. The chapter is concluded by a thorough literature review that follows this section.

After the introduction, core technical chapters begin with theoretical backgrounds of the core topics: storage systems and cyber security in chapter two. In chapter two, storage systems are presented in terms of its definition, history, basics and types. Cyber security of data storage is also presented in Chapter two. In addition, important terminologies are introduced including cyber security framework, risk triad and storage security domains.

After presenting the theoretical background of storage systems and cyber security and before assessing the use of local and cloud storage, cloud computing is introduced in Chapter three. The introduction of cloud computing includes cloud definition, types and models and characteristics. The chapter is concluded by an overview of cloud architecture, infrastructure, challenges and future of cloud computing.

The chapter that comes after the theoretical background chapters is chapter four in which local storage systems assessment is proposed and assessment proposal implementation on two organizations are presented. Full representations of assessments are appended in Appendix A, Appendix B and Appendix C.

Chapter five consists of two major parts. The first part correlates cyber security and cloud computing storage services and the other part presents the proposed solution to be considered by organizations that is based on a secure utilization of cloud computing for storage services.

In Chapter six, a conclusion of the thesis is presented follows by references and appendices.

Chapter 2: Theoretical Background and Literature Review

2.1 Definition of Storage Systems

2.2 History of Storage Systems

2.3 Storage Systems Basics

2.3.1 Major Computer Storage Categories

2.3.2 File System

2.3.3 Memory Access Methodologies

2.3.4 Block and File level storage access

2.4 Storage Systems Types

2.4.1 Direct-Attached Storage DAS

2.4.2 Network-Attached Storage NAS

2.4.3 SAN

2.5 Cyber security Framework

2.5.1 Confidentiality

2.5.2 Integrity

2.5.3 Availability

2.5.4 Other Properties

2.6 Risk Triad

2.6.1 Assets

2.6.2 Threats

2.6.3 Vulnerabilities

2.7 Storage Security Domains

2.7.1 Securing the Application Access Domain

2.7.2 Securing the Management Access Domain

2.7.3 Securing Backup, Replication, and Archive

2.8 Literature Review

Chapter 2: Theoretical Background and Literature Review

This thesis concentrates on the evolving topic of cyber security in different storage systems. It is worth to begin the thesis with a chapter that describes storage systems and cyber security and give a background on various aspects of interest.

In this chapter, a review of literature that is related to the subject of interest of this thesis is presented. Then storage systems are defined. A brief historical perspective is discussed before the thread goes into the basics and later the types of storage systems. After that, Specific types of storage systems that are based on application is explained before a conclusion to storage system that is the system concerned in this thesis.

After that an overview of the topic of cyber security is presented. The cyber security literature has been looked into from data storage orientation and that is how it is presented in this chapter. Cyber security framework is introduced followed by a thorough discussion of Risk Triad and Storage Security Domains. These three terms are the meat of cyber security sections in this chapter and creates a very good understanding as a background to the assessment chapter that follows.

2.1 Definition of Storage Systems

Storage in Computer Systems is normally referred to as a set of computer components and media that forms a technology that is able to keep digital data.

This technology nowadays is of different forms, one of which is a functionality form that is core in all of computerized systems. All computer systems need to boot from a memory into which the main boot program is stored (Ahmadi & Maleki, 2010).

Although Storage devices have different types and different purposes, the focus in this thesis is on non-volatile storage systems used for data storage and retrieval. For example, volatile memories may be discussed in a glance in this thesis but will have no focus due to the fact that it is irrelevant to the topic of the thesis. In particular, enterprise storage systems are the main focus over consumer storage devices.

It is worth to say as an introduction that the importance of storage systems comes from the fact that storage holds the crown jewels of every organization and is always a bottleneck of performance in almost all systems that an organization has. In addition, storage systems mostly are a cause of the longest lasting and most expensive failures.

2.2 History of Storage Systems

The main driver behind the continues development in the data storage technology field is the ever-increasing demand for storage capacity. In addition to capacity, other characteristics of storage such as operating speed, latency, and economics were addressed also in the evolution ladder (Goda & Kitsuregawa, 2012). Figures (1) and (2) present the evolution of data storage systems.

As paper was the most efficient storage media before computers after the old ages' clay tablets and wood strips, the first thing came into a human mind thinking about a storage media for computers was paper also. Thus, punch card has been developed to be punched (Mathur & Nishchal, 2010). Magnetic tapes have been invented and developed through a number of stages that has started with sound and later video recording. Optical disks practically have been announced in the 1980 with the first Laser Disk (LD). This type of disks became very popular for audio and video applications similarly to the first usage of magnetic tape drives (Ahmadi & Maleki, 2010).

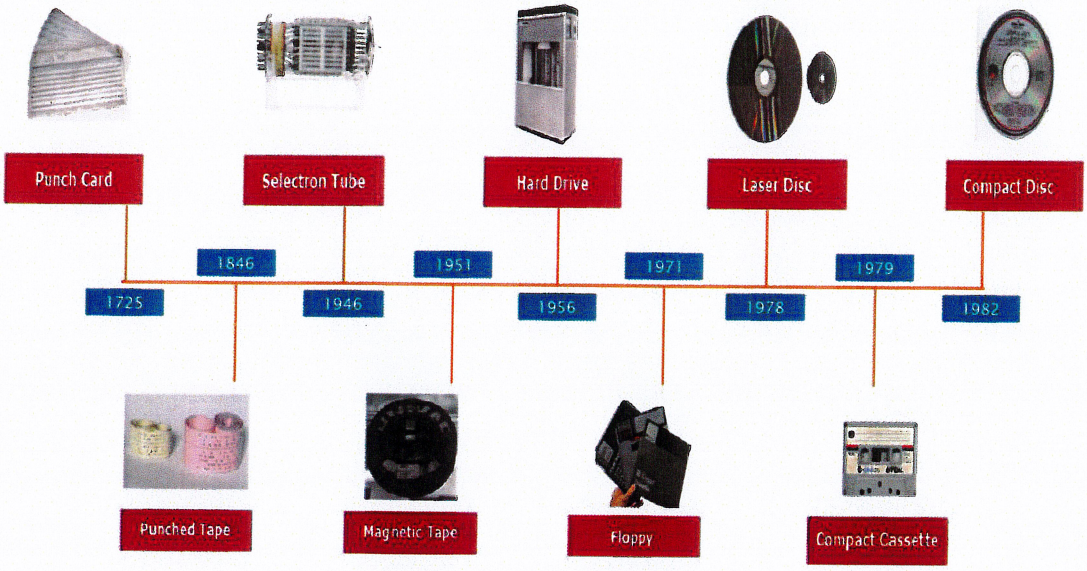


Figure (1)
Evolution of data storage systems (ODSI, 2014)

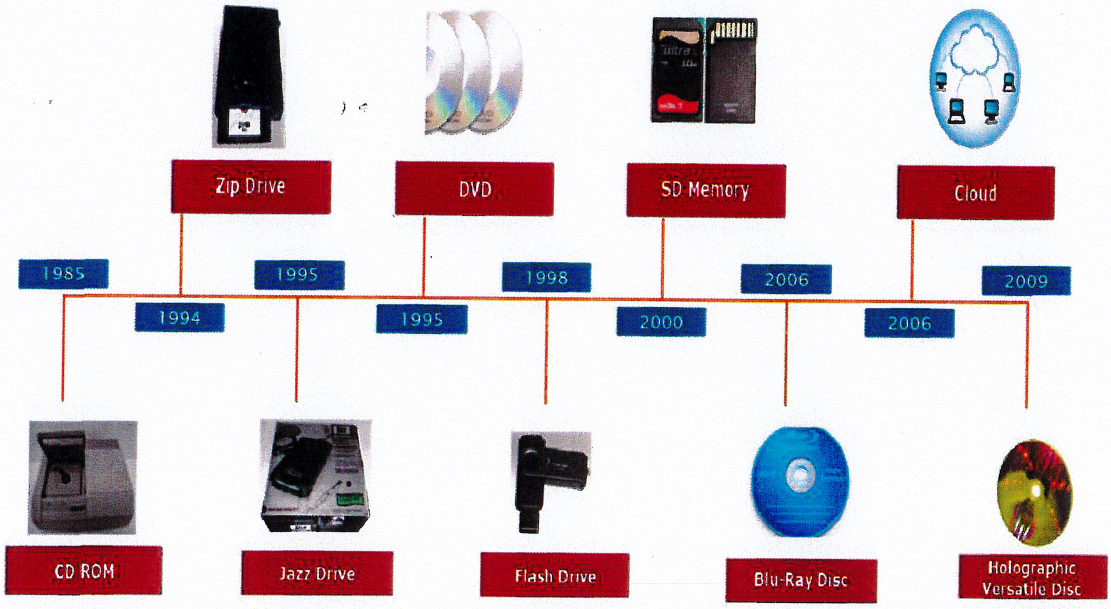


Figure (2)
Evolution of data storage systems (ODSI, 2014)

Although Flash technology is the most popular among others, especially after the big demand in the market for such memories that started in the 2000s (Goda & Kitsuregawa, 2012). Flash is a type of the Electrically Erasable Programmable (EEPROM), Read-Only Memory class of memories. Some widely used flash memories are Secure Digital

cards (SD) and compact flash memories. The recent evolution on which many big names in the IT industry are counting is the Solid State Drives (SSD) that uses flash memories with controlling circuit packed together.

Storage systems had several administrative and management challenges. Direct Attached Storage (DAS) is the terminology used nowadays to reflect the types of Storages that has a direct interface to systems (Goda & Kitsuregawa, 2012). Another category of storage systems has become popular after the rapid development of computer networks. The Storage systems of this category are referred to as Network Attached Storage (NAS) in contrast to DAS. The developments and enhancements in the NAS category of storage systems are following the development and enhancement in the computer networks (Riedel, et al., 2002). Elements like wireless networks, growing bandwidth, distributed intelligent protocols are all tracks of developments in networks and in NAS devices well.

Along with the arising of the storage networking, Virtualization was another technology that arises to address the distributed physical storage containers that are either resides on one system or scattered among a number of systems (Bilski, 2007). Storage virtualized technology was to build a virtual storage environment from a resource pool of storage devices. Storage virtualization is mentioned, it reflects the definition of virtualization of multiple storage devices into an array of disks unless it is explicitly defined.

Another major area of IT evolution in the last decade is cloud computing. Cloud computing is a term that describes a number of computer technologies and services. One of these technologies is cloud storage as a remote storage service that is provided by dedicated data centers that are managed to provide such services.

2.3 Storage Systems Basics

In this section, some basic terminologies that are essential for the area of research are described.

2.3.1 Major Computer Storage Categories

All computers and almost all digital devices have a storage hierarchy in which there are two main categories of storages.

The first is the fast type of storage that is small in capacity as well. This type of storage is volatile (It loses data when it is powered off) and is normally called Memory. Memory is relatively expensive and serves the CPU of computers by processing the live continues changing data required by the running operating systems and applications. Memory for the reasons mentioned is located typically near the CPU (Goda & Kitsuregawa, 2012).

The second is in contrast slower, larger, nonvolatile and cheaper. This type is normally referred to as storage. This storage category is the one of concern in this thesis.

2.3.2 File System

File system is the methodology computers uses to store files and retrieve them. The file system manages things like what sizes of chunks the data should be separated by and how to address each piece (Miller, et al., 2001).

Examples of files systems are File Allocation Table (FAT), FAT32, New Technology File System (NTFS) and Resilient File System (ReFS) for Windows. Macintosh systems support Hierarchical File System (HFS+) and Unix File System (UFS). For Compact disks and other

optical Medias such as DVD and Blu-ray, ISO9660 and Universal Disk Forma (UDF) are common file systems (Miller, et al., 2001).

2.3.3 Memory Access Methodologies

The ways of locating data falls into three categories as follows (Riedel, et al., 2002):

Addressed memory is the most used among different types of memories and file systems. To retrieve a data in an addressed memory, the address of the data is required.

The other methodology is the Associative memory; the part of the content is used to address the content. This part is called the mask in some protocols literature and is mainly used in cache memories.

The third methodology that is common in some storage medias such as tape drives is the **Sequential Memory**. In this methodology, data is addressed based on an offset of the position of the reader/writer head. The addresses in this type are always an offset in reference to another position.

2.3.4 Block and File level storage access

The previous section has explained the methods in which the data is addressed in the memory whereas this section describes the basic elements of storage access.

Block-level access is the basic method for disk access. The data is accessed in this method using block logical access. Block-level access is versatile and flexible in the sense that it can be used for almost all types of applications and storage requirement depending on how the volume configured on the disk is formatted (Ahmadi & Maleki, 2010). Block-level access storage is in the basic user friendly language a blank hard drive.

File-Level access is an abstraction of the basic access block-level. It is even built upon block-level access storage, but it hides its complexity. It is so simple to the extent that it is only a place to dump files. This type of access is not flexible and has only certain common protocols as configured to access (Ahmadi & Maleki, 2010).

2.4 Storage Systems Types

In this section, the major categories of storage systems are discussed. This includes DAS, NAS, SAN and virtualized storage.

2.4.1 Direct-Attached Storage (DAS)

Although storage systems that are directly connected to networks are very popular and have dominated in many applications. Storage systems that are directly connected to computers are still dominant for local data storage and small scale applications; those storage systems are termed DAS (storage systems that are connected directly to networks).

The architecture of DAS is basically a computer that can be a server or workstation, the storage media such as magnetic disks/disk arrays unlike network cables or devices that connect network storages to other servers and stations (Stanton, 2004). Host Bus Adapter (HBA) is an integrated circuit connection or adapter or in other words an electronic circuit that provides not only the physical connectivity between the storage media and the computer but also the storage/retrieval processing as shown in figure (3).

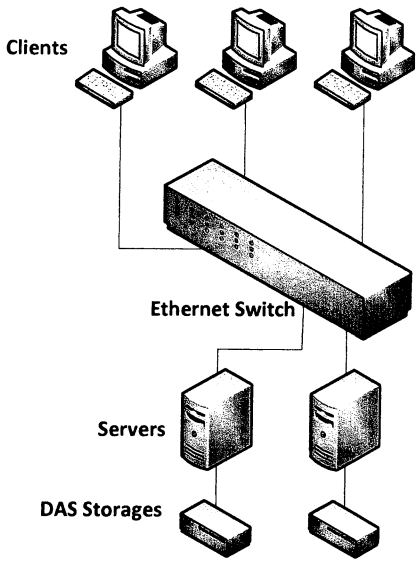


Figure (3)
A Sample Architecture that utilizes DAS Storage in a small network

There are two fundamental facts that complement the definition of DAS. The first one is that a DAS device has an external type that is connected to one computer like hardware Redundant Array of Inexpensive Disks (RAID) disk arrays and removable Small and Medium Businesses (SMB) medias.

The second fact is that DAS can be used by computers other than the one directly connected to by sharing the resources of the hosting computer (Riedel, et al., 2002).

2.4.2 Network-Attached Storage NAS

As the name implies, NAS is a storage system that is connected to a network. It can be accessed by devices connected to the same network that have the required access privilege. The glossy advantage of this type of storage system is the consolidation and single storage system for a network instead of multiple file storage servers or islands of data located on servers DASs systems (Moyo, et al., 2013).

Some of the file-sharing protocols that are common in NAS storage systems are Network File System (NFS) and Common Internet File

System (CIFS). As the NAS is independent upon the operating system that relies on users' computers, UNIX systems use NFS protocol for file sharing and Windows uses CIFS among other protocols that are usable with NAS. NAS devices are also run by an operating system that meets the needs and design of the storage system.

Centrality, Efficiency, Scalability, Availability and simplicity are only some of the features that are provided by NAS storage systems (Moyo, et al., 2013). Flexibility is an advantage in the sense that the NAS can be compatible with couple of industrial protocols and this turn into compatibility with multiple operating systems (Moyo, et al., 2012). At the same time, a drawback of NAS is its inflexibility in the sense that it cannot be configured to be something else like the block-level access DAS or SAN as will follow. The architecture of NAS is so simple and is shown in figure (4).

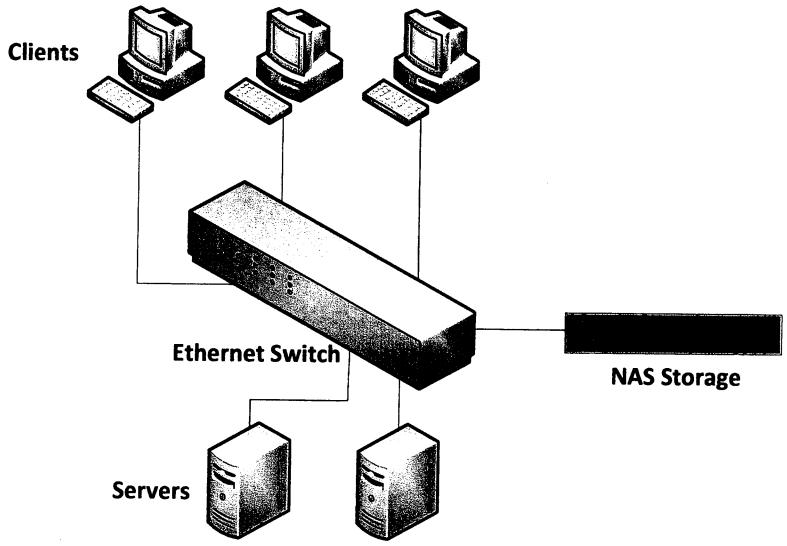


Figure (4)
A Sample Architecture that utilizes NAS Storage in a small network

NAS is also called by researchers and in some literature and industrial manufacturers personal cloud storage because of the similarity in several aspects. The fact is that NAS has paved the way to cloud storage systems (Sadiku, et al., 2014).

2.4.3 Storage Area Network SAN

SAN is an external storage array that is directly connected to more than one computer (Moyo, et al., 2013). The array of storage devices is a network by itself and that is why it is called SAN but it has no network connectivity to the computers utilizing it unlike the NAS devices.

SAN is based on block-level access disks. The famous applications for which SAN is almost always the best option is backup and recovery applications. In addition, the utilization of fiber channels allows a long distance between the SAN and the computers that are using it and this distance is very important for some disaster recovery procedures into which the backups should be located far away from the backed up stations (Kennedy & Gopal, 2010).

SAN essentially consist of dedicated network that is either fiber or copper depending on the application and requirement for storage medias as can be seen in figure (5). This network is separated from the network on which the servers or stations that is going to use the SAN rely on. The SAN can be even used to serve computers on multiple networks. Each and every computer that needs to utilize the SAN has to be connected through a fiber channel to the SAN network.

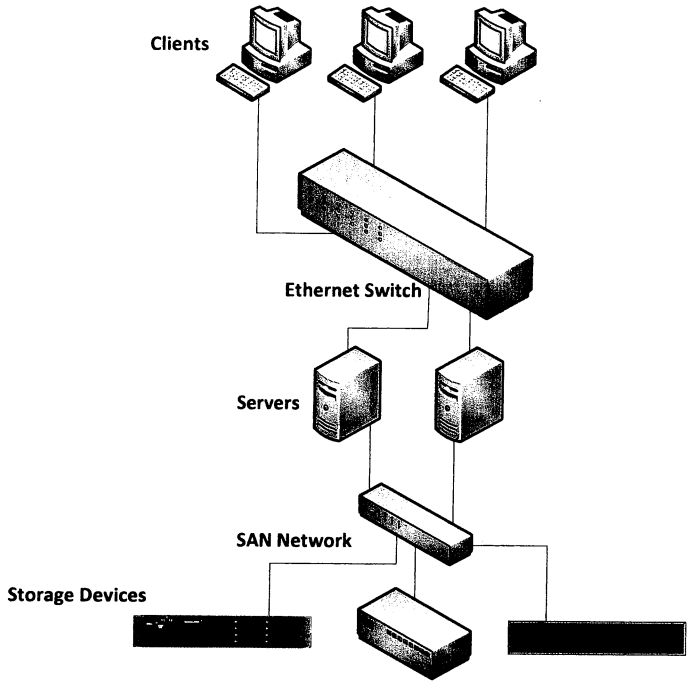


Figure (5)
A Sample Architecture that utilizes SAN Storage in a small network

IP SAN and FC SAN

IP SAN is a new SAN that is based on the Fiber Optic SAN (FC SAN) as it has been called after the introduction of the IP SAN. The only difference is that the IP SAN uses Transmission Control Protocol (TCP) and Internet Protocol (IP) instead of the fiber optic channels in its interfaces to hosts (Wang, et al., 2009).

The protocol that is used in the IP SAN products is Internet SCSI (ISCSI) mostly which is the same SCSI protocol that is used for DAS magnetic disks interfacing but running or communication over TCP/IP channel (Wang, et al., 2009).

2.5 Cyber Security Framework

After the thorough discussion of Storage systems in previous sections and to have the whole picture clear before presenting the assessment of storage systems in the organization considered in this thesis, an overview of the topic of cyber security is presented as well. The

cyber security literature has been looked into from data storage orientation and that is how it is presented in this chapter. The basic question that comes into mind when cyber security is mentioned is what to be achieved? Or what to be protected or prevented as security is a key term?

In cyber security, the framework is built to accomplish three major targets (Riedel, et al., 2002). The three are the CIA (Confidentiality, Integrity and Availability) and are also called in literature the cyber security triangle as shown in figure (6). Some other literature adds other properties such as accountability, non-repudiation and reliability as other goal to achieve by the cyber security framework.

According to the ISO standard ISO/IEC, information security is "Preservation of confidentiality, integrity and availability of information. Note: in addition, other properties, such as authenticity, accountability, non-repudiation and reliability involved."

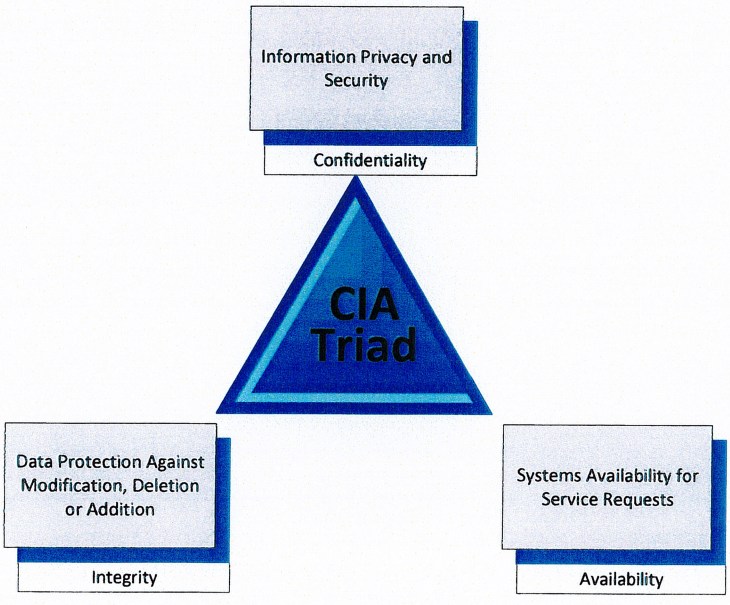


Figure (6)
Cyber Security Triangle CIA

2.5.1 Confidentiality

As the name implies, confidentiality is the secrecy of information. Confidentiality is a major goal of cyber security framework and is a challenge not only at the place at which the information resides such as storage systems but also at the communication and transmission links.

For information that resides on storage systems, authentication of authorized users is a key factor for protecting the information. In addition, encryption of data is another factor that keeps the information safe and confidential (Kennedy & Gopal, 2010).

Encryption is also a good measure for protecting the data that is in transit over communication channels. Additional protection for transit data includes hiding the management information of the data being sent including addresses of the source and destination and data amount and type of content.

2.5.2 Integrity

In simple terms, integrity of information is ensuring that it is as is and has not been changed. Authentication and proper authorization is again an important measure to ensure the integrity of the data in its residing location. For data in transit, error detection mechanisms that are part of the communication protocols can ensures the reliability and the integrity of the data (Stanton, 2004).

2.5.3 Availability

Availability is the accessibility of data for authorized and authenticated users at the time required. Many factors may disturb the availability of the data starting from attacks that keeps the data hostage busy such as denial of service attacks up to issues related to authentication (Stanton, 2004). This implies that the required resources

that makes the data available needs also a protection by the security framework.

2.5.4 Other Properties

In addition to the cyber security triangle (CIA), the International Organization for Standardization and the International Electrotechnical Commission (ISO/IEC) standard in its definition for information security declares a note. The note specifies other properties that are involved in the information security objectives such as accountability, non-repudiation and reliability (ISO/IEC 27000:2009). The following is brief explanation of accountability and non-Repudiation.

In order to maintain cyber security, each and every action should be logged with proper accountability. Deletion, addition, alteration and system configuration changes should be logged to track a cyber-security Incident (Kennedy & Gopal, 2010).

Repudiation is originally a legal term that has been used in the cryptography science and information security in reference to services and methodologies that is used to provide proof of integrity and origin of data. To make it clear in legal terms, if there is a dispute in a lawsuit it is possible to hold one party to their commitment using non-repudiation evidence (Kennedy & Gopal, 2010).

As mentioned earlier, some information systems are highly concerned of confidentiality of the data with lower importance of availability. For such applications where the information should not be revealed although it may need some time to be retrieved the security framework is entirely different from the framework required for another application that is highly concerned about availability and does not care about confidentiality because the data is raw for instance and needs a complicated applications, interpretation and expertise to be understood.

2.6 Risk Triad

A holistic way of risk identification is dividing it into three major arms, threats, assets and vulnerabilities. The threat is the acting factor that utilizes the existence of vulnerability in a system to compromise the security (confidentiality, availability or integrity) of the asset.

The important arm of the triad which organizations focus on is the vulnerabilities. All of the security hardening efforts by organizations is to close and minimize the vulnerabilities to make it very difficult for an attacker or a threat to access an asset and compromises it (Moyo, et al., 2013). Countries and governments sets rules and regulations to minimize the threats by setting and announcing penalties on human attackers and by also enforcing rules on organization to harden their systems and reduce vulnerabilities specially for systems of organizations that are of a national interest such as critical infrastructure organizations, national income organizations and governmental security departments.

2.6.1 Assets

Information is nowadays one of the most important assets. Different scales of hardware may construct storage systems that has a negligible value in comparison to the information importance and value that resides on the storage system. The assets that are related also to the information are also important such as the Hardware, Software and transmission infrastructure.

The storage system security measures and systems cost should be a fraction of the value of information that is stored on it and should also make attackers trials for compromising the security of the information more difficult and costly. In case of a failure in the security framework that yields to a loss of data integrity or availability, backup and replication is a very important measure for valuable assets although the

availability of a backup will never protect the confidentiality of an information that have been accessed or stolen.

2.6.2 Threats

Threat is the second arm of the risk triad, and it is the attacker that is the reason for which the security measures and frameworks exists. In literature, threats are classified as passive or active based on the way they act and the objective they target. For attacks or threats that are considered to be passive, the confidentiality is the target. An unauthorized listener to data or a backdoor program that sends copies of information to an external source is passive attacker (Microsoft, 2000) On the other hand, any attack that compromises other security measures (availability, integrity or accountability) is considered to be an active attack. An example of an attack that compromises the availability is a Denial of Service attack (DoS) as explained earlier when availability was addressed.

Any attack that modifies data is considered is an active attack that compromises integrity. For accountability, although the attacks that targets this property of information is rare but it is highly risky especially when information really matters for critical applications (Ateeq, 2012). Repudiation is a type of attack that works as a man in the middle. This attack acts differently from case to case, sometimes it performs actions and erases any evidence of the performing authority or it reveals wrong information when a request comes to a genuine data.

A very important fact to be considered is the fact that the major party that may be affected seriously and harmfully from the said attacks and threats is the storage system due to the fact the mostly data and information that resides there is of a considerable importance in some way (Ateeq, 2012).

In addition to the above mentioned classification which is repeatedly seen in literature another classification which is based on the nature of the attacker or threat in contrast to the nature of security measure that it compromises as the previous model suggests also exists in literature and discussing adds a value to the topic of threats.

Attacker or threat is not always as the name implies an entity that purposely trying to compromise the security of the data, it is also a natural disaster that may compromise the availability of the data or an ignorant employee unintentionally modified the data and compromised its integrity.

Figure (7) illustrates a simple classification of security threats based on the nature of the attacker.

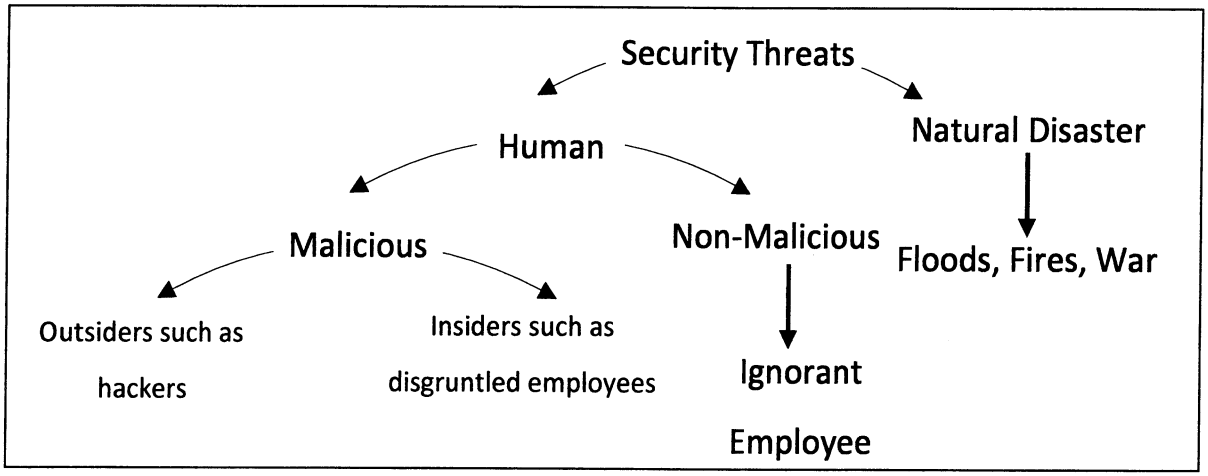


Figure (7)
Security Threats (Microsoft, 2000)

• ***Natural Disasters:*** Although such risks are very disastrous and can lead to major information loss, this category of threats is not discussed thoroughly in this thesis due to the fact that it is not the type of cyber security risk this thesis assesses. Natural disastrous such as earthquakes, fires, lightening and floods may compromises all of the cyber security measures (CIA and Accountability) and the class of mitigation differs from human attacks in the sense that cyber security techniques such as

firewalls, intrusion detection and other software and hardware equipment does not prevent natural disastrous. For such kind of an threat, other measures such as backup and replication, distributed systems, incident management, disaster recovery plans (DRP), and business continuity management (BCM) and emergency plans are the most effective and essential as well for information systems including storage systems.

• ***Non-Malicious Ignorant Employees:*** Recent statistics shows an important percentage of cyber security incidents are a direct or indirect cause of an ignorant employee. In a recent report released by the national security institute, it is declared that 75% of the security breaches are "inside jobs" Directly employees may delete files, or change configuration or even reveal confidential information. All of these mistakes may lead to catastrophic breaches and consequences (Microsoft, 2000). In addition to the direct mistakes that employee may perform indirect actions that help and paves the way to malicious attacks to happen is another kind of ignorant employee's common issue (Ateeq, 2012). Cyber security staff or storage system custodians for instance may not pay attention to a failure in the antivirus server that updates the virus definition for all of the virus scan agents on the computers; this will lead to a major vulnerability in all of the computers that allows for virus attacks.

Although there are many measures that is discussed, this specific type of threat is a major topic of discussion in this thesis because it is one of the most critical decision criteria for choosing to hire a well-established data center to host the storage systems relying on their dedication for data center maintenance or trusting the organization's local team and accepting a risk of an ignorant employee type of threat as well as inside attacker as explained in the next threat type.

• ***Inside Attacker:*** The ignorant employee threat has been said to be the most common but the inside attacker threat is always the most severe in impact and consequences. An inside attacker is firstly very knowledgeable of the system design, vulnerabilities and infrastructure. In addition, the inside attacker have a certain authorization that allows him to pass most of the boundaries that is designed to stop outside attackers (Microsoft, 2000). Those are not the only reason for being the most severe. Inside attacker knows very well what hurts the organization mostly in terms of data loss, resources and revealing confidential information.

All of the technologies implemented for cyber security is mostly targeting outside attackers. Policies and Procedures are also set to minimize the possibility of an incident due to an ignorant employee (Ateeq, 2012). Disaster Recovery and Business continuity plans and emergency backup locations, resources and information are set for the possibility of having a natural disaster. For inside attackers, there are no effective way to stop inside attackers other than some measures that may reduce the effect of an inside attack such as splitting responsibilities, reviewing privileges and spreading awareness.

• ***Outside Attacker:*** This is the type of attack that comes into minds when the terms attack, malicious attack, hacker, cracker and virus are mentioned. Cyber security teams and personnel spend most of their efforts in assessing and closing out vulnerabilities to stop an outside malicious attack (Microsoft, 2000). Measures and techniques are very diverse and have different flavors that are discussed from security domains perspective in short. The effectiveness of these techniques depends on proper understanding of the types of attacks that may happen and the aims and causes of attackers as well.

Historically hacker has referred to a people who are very knowledgably in computers and has a hobby and some skills in software and viruses and can penetrate his neighbors' computers. Crackers as well were people who can crack licensed software. Now hackers and crackers are very professional. And work for organizations and countries for financial reasons in tracking important information of future products of competitive organizations. Countries are also forming professional institutes and teams for cyber defense which is called cyber war. Malicious attacks are getting high importance due to the level of mass destruction that it can cause.

2.6.3 Vulnerabilities

In order to feel the spectrum of vulnerabilities in a system, storage system is taken as a model.

Vulnerabilities in Storage systems may reside in the storage data itself. Data or information assets that are in clear format and not encrypted are data with vulnerability and the attacker who manages to overcome other layer of defense and reached the data in a way or another will be able to understand or interpret it easily and use it directly. Introducing encryption that is difficult to break is another level of protection especially for data that passes through vulnerable media by nature such as public networks.

Vulnerabilities may also reside on the storage resources. The system and media on which the data is stored should be always under different levels of assessments. All types of Software starting from operating system and until unused applications and services that is installed in the storage system should be always updated with the latest available security patches (Ateeq, 2012).

In addition to data and storage system resources, network infrastructure should be always hardened against different vulnerabilities such as hardware obsolescence, unused open ports, and simple network management protocol (SNMP) communities that are not password protected and default passwords.

Physical security and maintaining secure access to the entire infrastructure associated with the data storage in addition to hardening the vulnerabilities of systems that are interconnected and interrelated with the storage system such as a central authentication server, Domain Name systems (DNS) or gateway systems are all of an absolute interest and requirement of cyber security (Ateeq, 2012).

The entire above yield to the conclusion that the spectrum of vulnerabilities is very wide and diverse and needs the collaboration of different teams in addition to strong policies and procedures that insures that mostly nothing is missed and all windows for attackers are closed.

2.7 Storage Security Domains

Storage system is a service system that services a number of users by enabling them to store and retrieve data. Such a system is required to be accessible on a network whether it is a DAS storage that is hosted on a server and the server is connected to that network or a NAS or SAN that is directly connected to a network (John & Tolga, 2000).

The network may vary in its size and may be connected to the internet or a Wide Area Network (WAN) depending on the application of this storage system. In all cases, the risk surface from which a security compromise can be initiated is proportional to the wideness of the network the storage system is connected to.

This does not mean that the risk surface should be minimized. Because this conflicts with the idea of being a storage service that should

be utilized to the maximum extent by the company or organization. The correct way to deal with the potential risk surface is to study it and introduce controls to ensure that every access path to the data is protected by a security measure that makes it not possible to be compromised (John & Tolga, 2000). In general security professionals categorize the access paths into three storage security domains (Alexander & Cowley, 2010): application access, management access and backup, replication and archive.

Security professionals assesses the three domains vulnerabilities and come with security measures and techniques that are integrated in a security framework to protect the confidentiality, integrity and availability in addition to the accountability in each of the three domains as shown in figure (8).

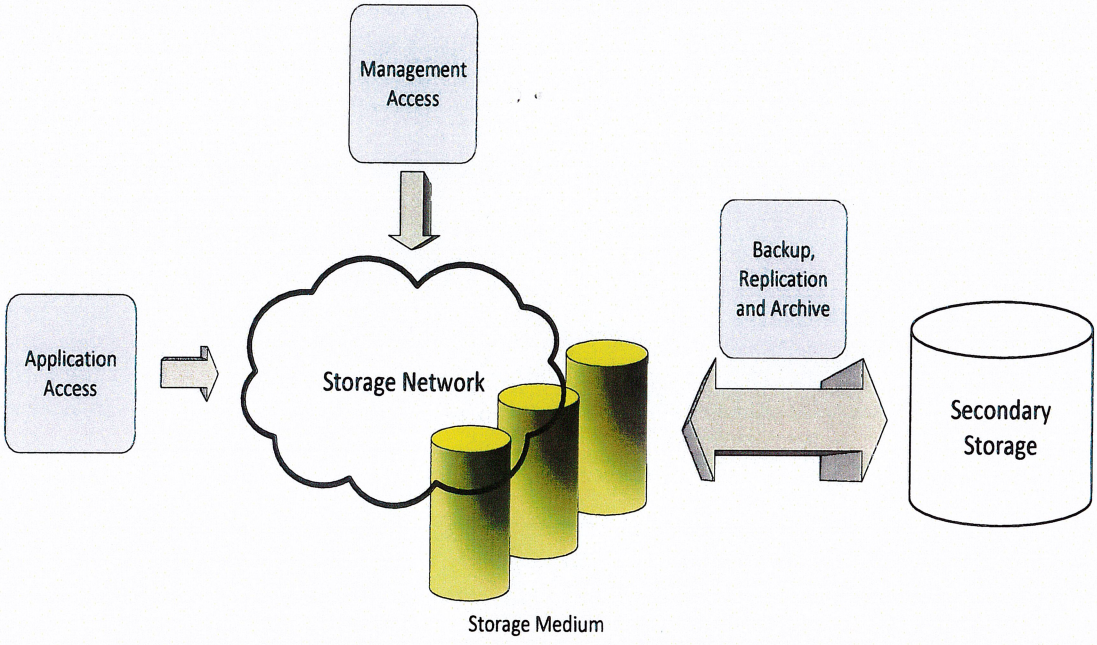


Figure (8)
Storage System Security Domains

2.7.1 Securing the Application Access Domain

As the name of application access domain implies, it includes application users that uses database interface, application client or file

system to access the data. As stated earlier, the application access domain should be assessed to introduce appropriate controls that prevent attacks from this domain.

As what is done in this thesis for the three security domains, figure (9) summarizes the access paths for threats for the domain by identifying it with a cross-sign and indicating the possible threat by explosive notation.

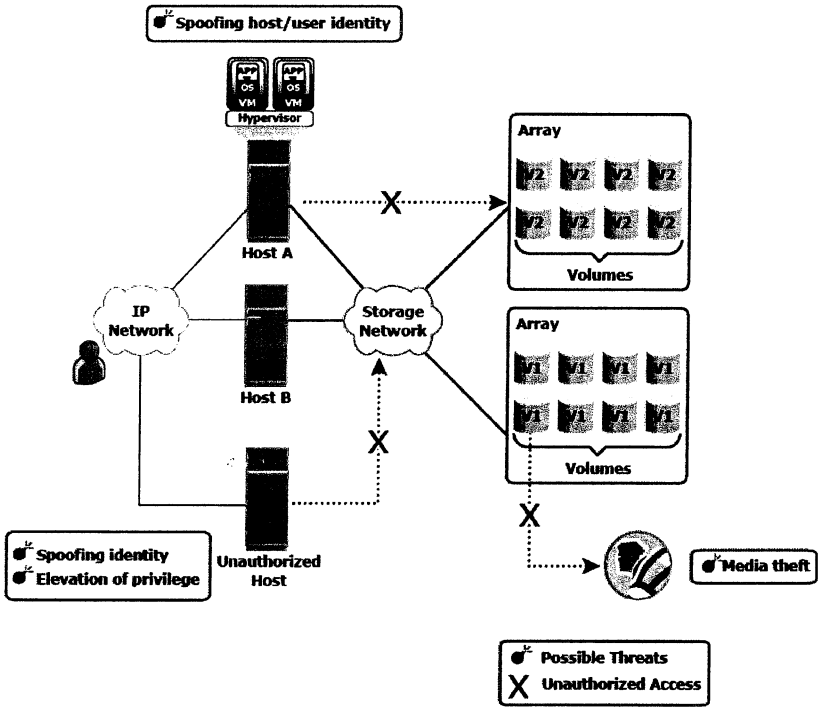


Figure (9)
Security threats in Application access domain (Gnanasundaram & Shrivastava, 2012)

The possible risks identified in the figure (9) and the unauthorized paths of access should be controlled by a set of security techniques. The following are the main security measures and controls for the access domain.

- ***Controlling User Access to Data:*** Authentication and authorization are always the controls that are imposed and regulated to ensure proper control over user access. Spoofing a host identity for authentication or for uplifting the authorization privileges is a

threat on the confidentiality and integrity of data (John & Tolga, 2000)

Examples of controls that protects users access to data are:

- Unified centralized strong systems are normally used for authentication, user privileges and group security policies. Windows server domain controllers are a trusted centralized authentication server that is used for millions of networks and domains all over the world. Central authentication mechanism can be integrated with other technologies and interface systems such as triple 'a' for authenticating other devices on the infrastructure such as network devices.
- Information rights management (IRM) is a content host level authentication system used by some NAS devices.
- Network zoning is a control mechanism on the data flow over the switches on the network.

Regular auditing is required to ensure that all controls are implemented. Checking logs and ensuring proper logging mechanism is also very important factor to assess accountability of all users' actions on data.

- ***Protecting the Storage Infrastructure:*** The data of storage can be accessed in transit on any of the transmission mediums. This risks the confidentiality, integrity and even the availability of the data. Data may be confidential and stolen through tampering the networking infrastructure and the cabling (John & Tolga, 2000). By accessing any of the network devices of the storage infrastructure data integrity can be compromised by modifying the data and a denial of service attack shall make the data unavailable. Examples of controls that protects storage infrastructure, (John & Tolga, 2000):

- Physical security control of the whole storage infrastructure. Any of the components that have direct access to storage infrastructure should be kept in an access controlled environment.
- Network data encryption protocols. Data flow should use protocols that have a certain encryption mechanism to assure its security over network.
- Introducing virtual local area networks (VLAN) over the network to separate different types of traffics specially management traffic that allows control over network devices.

- ***Data Encryption:*** After discussing normal data access for users and data flow on the storage infrastructure, what if data is stolen or tampered on its final location that is the storage system? Such an attack compromises the confidentiality and integrity of data. Examples of controls that protects storage infrastructure (John & Tolga, 2000),
  - Data encryption mechanism that encrypts the data before being stored on the storage system is an effective way of protecting the data. Encryption can happen at the host side or on any of the transmission stages before it reaches its storing destination.
  - Data retention policies and procedures ensures that data is not kept for a period of which it is not needed any more and attention to such data may deteriorate along the time causing it to be vulnerable for attacks.
  - Erasing mechanisms for data that prevent data confidentiality loss after getting rid of old hard disks and storage media.

- The usage of protocols that includes algorithms to check the integrity of data.

2.7.2 Securing the Management Access Domain

In the previous section the data access domain has been explored but the management access to the resources of the storage infrastructure is as important as the data access. Managing, monitoring and provisioning of the storage systems and resources require access to the management console of the storage systems and management software of other components of the infrastructure (Stanton, 2004). As done in the data access domain, figure (10) summarizes the access paths and possible threats to the management access domain.

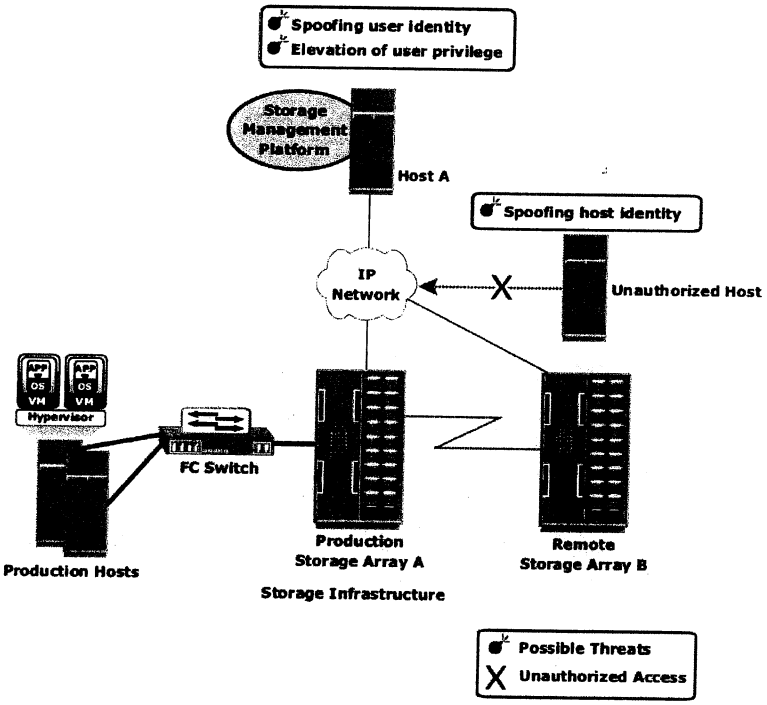


Figure (10)
Security threats in Management access domain (Gnanasundaram & Shrivastava, 2012)

The possible risks identified in the previous figure and the unauthorized paths of access should be controlled by a set of security techniques. The following are the main security measures for the access domain.

- ***Controlling Administrative Access:*** Controlling the administrative access is of no doubt more importance than user access. Because it affects not only the integrity of data but also the integrity of devices on the storage infrastructure. Examples of controls that protects storage infrastructure are: (John & Tolga, 2000)
    - External professional authentication directory such as Active directory.
    - Policies and Procedures that enforces roles splitting and minimizes Administrative privileges to the least required for the job.
    - Auditing security logs continuously and ensuring by technology means that the logs are accountable and synchronized by time for incident investigation and are protected as well. This may be achieved by having a centralized time server and centralized security monitoring facility.
- ***Protecting the Management Infrastructure:*** Availability of management access is as important as protecting it from spoofing and snooping as well. Accessing the management infrastructure allows monitoring SNMP traffic for instance as well as other management traffic that includes sensitive information that allows exploiting the whole system and resources (Alexander & Cowley, 2010). Example of controls that protects storage infrastructure is splitting the management network from the data network by physical routers and logical networks over level 2 network devices.

2.7.3 Securing Backup, Replication, and Archive

Backup, replication and archives are very essential part of recovery and emergency plans. No organization can sustain without a recovery

plan for any information incident or disasters. Having that said, the backup itself is a potential risk because it contains all of the information that is available on the original system.

The risk surface is again based on the method and the software that performs the backup or replication. If the backup is done directly to a remote site the risk surface is wider than doing it locally only but doing it over sites is essential for the business continuity plans (John & Tolga, 2000). The backup software and the protocols it uses also affect the security of such a process. Organizations need to ensure that the level of security of the backup and replica of the systems is of the same level as the original system.

Figure (11) presents the access paths and possible threats to the backup environment.

The model presented assumes a remote disaster recovery (DR) site. The threat of spoofing the identity of the DR site and initiate a backup session to the attacker is a common risk that requires security measures. The attacker may also utilize that spoofed connection to compromise the availability and integrity of the data on the original system.

The tape backup or any other type of media should be security monitored and assessed as well. Data should be encrypted before written on such media devices that are vulnerable to be stolen because of the nature of easy handling of them.

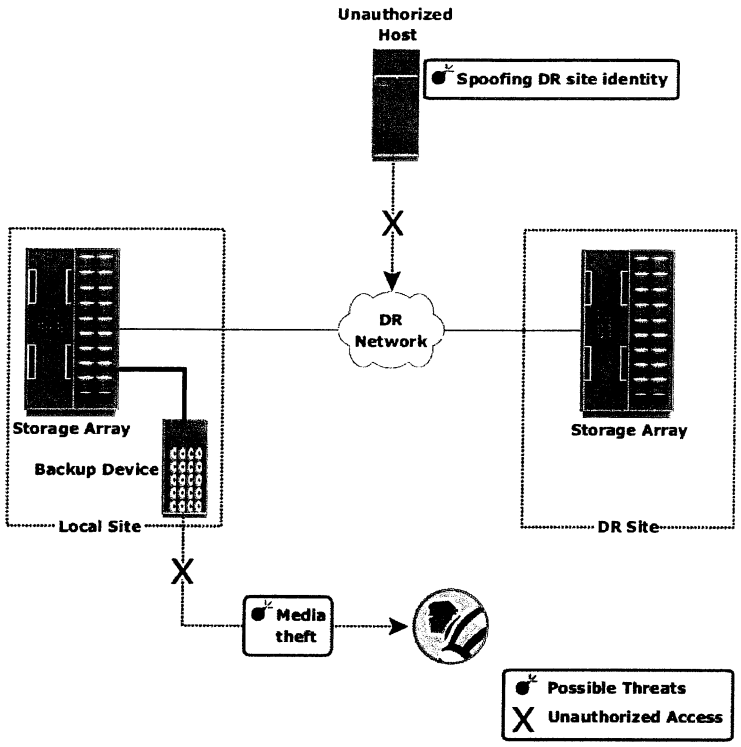


Figure (11)
Security threats in the Backup domain (Gnanasundaram & Shrivastava, 2012)

2.8 Literature Review

The big transition which has happened in the last decade from paperwork to electronic work and from manual operations to automatic is because of the heuristic magnificent development in computerized systems. Nowadays, many computerized systems and components are a must for any organizational operations. Examples of such systems are: databases server, mail server, web server and storage server. Storage systems which are systems of interest in the research of this thesis are one of the most important, if not the most, because the whole data that other systems are dependent on resides in it. For this reason, storage systems has evolved rapidly in terms of storage medium, architecture, communication protocols, encryption ...etc. Storage systems attracted many authors; they studied their evolution, types, features, access techniques, and architecture (Goda, K., & Kitsuregawa, M. 2012).

Moreover, securing the storage system is one of the important issues which have been studied by many researches such as Ateeq (2012) because of various security attacks and threats. Therefore, developing security systems to protect the storage systems are needed. A number of researchers have studied the security of storage systems and they proposed different solutions to solve the problems of securing storage systems (Miller, et al., 2001; Stanton, 2004).

In order to improve the security of a system, we have to assess the current security system. The author Stambul, M. in 2011 has suggested an assessment model for information security. Authors concluded that the model they have suggested can be used by organizations to assess the level of maturity of the cyber security framework of the organization. Another paper (Usman & Ayub, 2012) has suggested a policy architecture that can be used for complete control and better governance of cyber security. Riedel et al. (2002), have proposed methodology for evaluating storage systems based upon certain cyber security aspects is presented. For this reason, two axes have been the basis of the evaluation: performance axes and security axes.

Cloud, on the other hand, one of the approaches to implement storage systems, has been studied by many researchers presenting cloud technology as networks of the future. They introduced, analyzed and presented a robust research covering well established cloud providers that are offering cloud services to the public. For the reason of computing capability when utilizing cloud computing as a technology, authors suggested cloud as being a major step in the computing spectrum and performance (Koletka & Hutchison, 2011). Furthermore, cloud security has been investigated by a number of researchers. Wang et al. (2009) have presented certain methodologies to enhance and fill gaps in the cyber security models of storage services offered by cloud providers. Liu

(2012) announces some cloud computing systems and investigates cloud computing security issues and its approaches according to the cloud computing features and concepts. Also the paper illustrated a cloud conception and verified the cloud abilities such as scalability, elasticity, platform independent, low-cost and reliability. The security issues in the cloud system also have been studied.

In this study, the traditional storage systems is assessed and audited from security point of view, by identifying clearly the current security threats and risks. After that, different techniques and solutions which are needed to harden the security of the server and close the vulnerabilities available are studied. Using the cloud storage services as an alternative technique is assessed as well in this study. In addition, the security effects in particular of such a transition are studied. The first part will be about how the transition will affect the current threats which has been concluded from the study, and the second is the new security risks which will be introduced because of the transition. Finally a whole secure cloud storage system design is proposed based on security techniques that is related with the introduce security threats.

Chapter 3: Cloud Computing

3.1 Definition of Cloud Computing

3.2 Cloud Types and Models

3.2.1 Deployment Models

3.2.2 Service Models

3.3 Cloud Computing Characteristics

3.3.1 Advantages

3.3.2 Disadvantages

3.4 Cloud Architecture and Infrastructure

3.5 Challenges and Future

Chapter 3: Cloud Computing

Cloud computing is the evolution of IT systems that promises enhancements in cyber security as well as other IT concerns. Before discussing the effect of migrating storage services to cloud on current cyber security concerns and the new security vulnerabilities and worries it arises, this chapter is an introduction to the topic of cloud computing that paves the road to the following chapter that interrelates cloud, cyber security and storage systems.

This chapter starts with defining cloud computing. Cloud types and models follow the definition. These types and models that are basically the deployment and service models are considered to be part of the definition and that's why they are discussed right after the definition of cloud computing.

After that Characteristics that are considered to advantage or drawbacks are discussed. The chapter ends up by presenting the architecture and infrastructure of cloud computing in brief and concluding by highlighting the future and challenges of cloud computing technologies.

3.1 Definition of Cloud Computing

Cloud computing is a term that refers to IT model of providing computing resources and services such as networks, servers, storage, applications, or service through any type or size of computer network or the internet (Antonopoulos & Gillam, 2010). Other definition for cloud computing is "Clouds are a large pool of easily usable and accessible virtualized resources".

Different researchers adds additional information related to cloud computing to the definition such as the service models and deployment models that it has which is discussed in the following section. Others add

some features that are an integral part of the idea of cloud computing such as the ease of expanding utilization domain (Rapid Elasticity) and the minimum management efforts required for maintenance (Antonopoulos & Gillam, 2010).

3.2 Cloud Types and Models

Cloud models are differentiated based on service purpose and capacity and security requirements. Deployment model and Service model are two characteristics that identify many specifications of the cloud service required. The following summarizes the model options of the two categories.

3.2.1 Deployment Models

There is several deployment models defined in literature. Deployment model reflects the management, service delivery and customer class characteristics of a cloud service. The following are the most common models (Jansen & Grance, 2011):

- ***Public Cloud:*** A public cloud is a cloud that is available for consumers on the internet. It services a very wide range of customers with different requirements and service scales. Personal use of public clouds is the dominant usage of this type of clouds.
- ***Private Cloud:*** Private cloud is the ultimate opposite of public cloud. It is a cloud that is exclusive for one organization .Having this said, this cloud can be operated by third party and can be located also at a datacenter that is outside the organization's facility. Whether a private cloud is maintained by organization's staff or third party, the organization has full control and management over the cloud infrastructure .Public and private are the two limits of a wide spectrum of deployments. The next

deployments, community and hybrid, are different ranges of that spectrum.

- ***Community Cloud:*** Community cloud is similar to a private cloud, but instead of serving only one organization it is designed for two or more organizations that are normally part of one government or one corporate or have certain type of bounds.
- ***Hybrid Cloud:*** As the name implies, hybrid cloud is a mix of clouds using the same infrastructure. In this case the cloud infrastructure may serve single organizations with private cloud in addition to having a spectrum of public services.

3.2.2 Service Models

Service model is another key characteristic of cloud as deployment model is. Service models are independent from deployment models. In other words, each service model can be provided using any deployment model. The following are the basic service models used in the cloud industry.

- **Software-as-a-Service (SaaS):** Software-as-a-Service is a model of service into which applications and resources required to run the applications are delivered to the customer (Dawoud, et al., 2010). Customer has a limited management privileges in this model such that only application preferences can be changed as a profile. All other resources hosting applications and supporting it is transparent to the customer and the customer has no access to it by any means.
- **Platform-as-a-Service (PaaS):** Platform-as-a-Service is a broader model of service that provide a computing platform on which applications can be established and deployed rather than providing applications only. The customer in this model has as expected higher privileges and can access settings of applications and the

platform hosting the applications (Dawoud, et al., 2010). This transfers more responsibilities from the cloud provider shoulder to the cloud customer.

- **Infrastructure-as-a-Service (IaaS):** Infrastructure as a service is the highest servicing capacity model in the pyramid. It provides all of the components of an IT infrastructure such as networking, hardware, software, and equipment resources (Dawoud, et al., 2010). The user in this model has a high factor of freedom in configuring the virtualized service he got through a service interface the way he wants.

Figure (12) visualizes the cloud services layers of responsibilities, access and management. The first column to the right is the Software-as-a-Service model where almost everything is managed by Cloud vendor except probably application preferences and profiles.

Everything starts from the application down until the physical infrastructure and hosting environment. When a higher level of service is acquired from a cloud vendor that includes the resources needed to build an application, the cloud service is named platform-as-a-service as explained earlier (Dawoud, et al., 2010).

The Platform-as-a-Service, as visualized in the second column from the right in the figure, includes compilers, libraries and all operating requirements that allows a specific application to run and that is why specifying the type of applications that requires the service is a key when platform-as-a-service is required (Koletka & Hutchison, 2011). Referring again to the figure, when a service steps from platform-as-a-service to infrastructure-as-a-service, runtime, middleware and operating system are added to the package but over a virtualized environment.

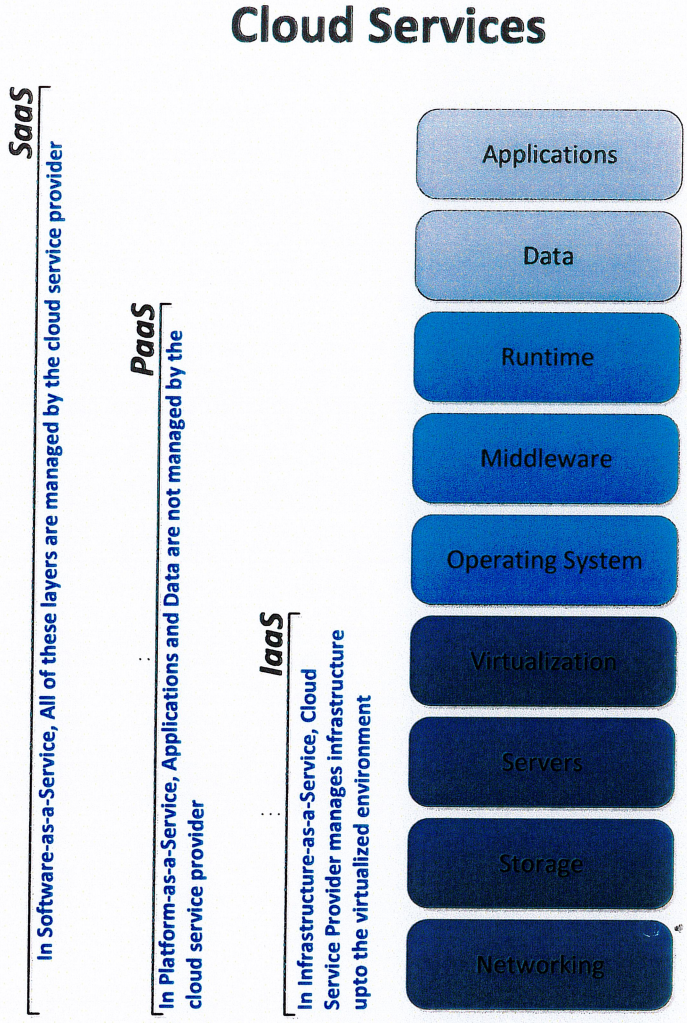


Figure (12)
Cloud Service Models

The virtualization layer includes all the stuff related to the virtualization technology like hypervisors and virtual hardware and data like network, storage and machine (Sitaram & Manjunath, 2011). This shows clearly that even when Infrastructure-as-a-Service is required, the infrastructure is virtualized and the responsibility of managing the actual hardware and hypervisors software is on the cloud vendor all the way down to the facility and the environment into which the hardware exist such as the HVAC system, safety systems, power distribution .. etc.

3.3 Cloud Computing Characteristics

Any decision maker in an organization needs to understand a new technology from all of its aspects before taking a decision in the feasibility of acquiring the technology to the organization. Migrating to cloud computing is such a big decision and strategic movement that requires high attention to benefits and drawbacks of such a change (Koletka & Hutchison, 2011). The following are the major benefits and drawbacks of cloud computing and a brief description of how this characteristic is classified in this category and why.

3.3.1 Advantages

The following is a list of some of the advantages of utilizing cloud computing.

Cost

Cost is the most apparent and clear benefit from using cloud computing services. Obviously there will be cost elimination of hardware, software, upgrades, maintenance staff, spares, licenses, support contracts, and environment utilities ...etc.

In addition, it wouldn't be possible to have a system that is optimized for the need of the organization and the capacity of the system will be overestimated and the resources are wasted or under estimated and the cost of increasing the capacity will be higher than having a high capacity system in the project phase. A good statistic that gives an indication of the problem is the one published in the IEEE computer society magazine and states that most enterprise datacenters utilizes less than 50% of the capacity of their systems (Mathur & Nishchal, 2010).

On the other hand, cloud services has a cost but is generally less expensive than in-house systems regardless other benefits and drawbacks of cloud services. Another point related to cost is the transition of IT

services budget from being (CAPEX), Capital expenditure, budget to (OPEX), operating expenditure. Organizations are in favor of reducing CAPEX expenditures because of the front-loaded nature of such budget in addition to being subject to depreciation.

Efficiency

As stated in the last paragraph, in cloud computing a consumer estimates exactly how many resources required for the applications and set the service contract on that basis. If the demand increases, it is very easy to ask for more resources from the cloud service provider because of the modularity and nature of cloud infrastructure (Mathur & Nishchal, 2010).

In comparison, that is not applicable for in-house installations. Organizations will have either to over-estimate and assume a big margin for the resources in such a way that prevents them from upgrading the systems very quickly and before getting the suitable return from the investment done. Otherwise an organization might target efficiency but limits the flexibility it has in adding systems, function or even users (Mell & Grance, 2011).

Flexibility

IT systems are such systems that are very volatile and evolve in no time. In addition, consumers are becoming very much interested in new technologies that help in enhancing the businesses of the organizations. For these reasons, capacity for new systems and software is required always without the ability to predict the time in which it is required and the size of the capacity required as well.

Upgrades of in-house installations are not easy and the time it requires is not predictable. On the other hand, cloud computing is a modular service that is easily expandable and resources are always available for any kind of application (Mell & Grance, 2011).

In addition to this fact, normally hardware is designed to suit certain software and operating systems. Operating systems always have major upgrades in a span of couple of years and that in most of the cases requires hardware upgrade for best compatibility and performance. Cloud computing excel in flexibility because of the design of the systems in service provider data center.

Availability

Stating availability as an advantage is regardless the fact that the availability may be affected by organization to consumer interface and the reliance of this service is dependent on the communication channel between the provider and the consumer.

Assuming that the communication channel is reliable and have all the means of redundancy and resilience, the availability of cloud services is better than the availability of in-house systems because of the large scale system that have bullet proof protection, recovery, monitoring and maintenance capabilities (Mathur & Nishchal, 2010).

Environmental Friendly Solution

Most of the companies, organizations and governments have to show certain responsibility to global warming issues and environment in general. Utilizing cloud computing is a "Green" step because of couple of reasons: The first reason is that it is efficient to operate one data center instead of operating single installations on consumer facilities. The second reason is most of the prominent cloud service providers nowadays uses power efficiently and have certain low emissions systems in place (Mathur & Nishchal, 2010).

Security

Security issues are left to chapter six which discusses in details the security benefits and drawback of migrating to cloud. But it is worth to mention that cloud computing has significant security advantages in

addition to the drawbacks that it brings. This information is missed from a number of literatures that assumes that although there are benefits from migrating to cloud but always there is a compromise in the cyber security side.

3.3.2 Disadvantages

Although most of the characteristics advantage and disadvantage is a relative correlation and depends on the organization and the method it utilizes cloud services but the characteristics that are stated here and the explanation given is a conclusion of a research in cloud characteristics of a tremendous number of literature books and articles.

Control

A decision maker with a confidentiality oriented mind will never allow a step towards cloud computing because eventually not only the data of the organization is out of the premises of it but also the control over the infrastructure that provides the service (Sadiku, et al., 2014).

This drawback is corner stone feature of cloud services because the idea of cloud services is to outsource the infrastructure control and management of IT systems. Loss of control is also discussed in chapter six as a security issue because it affects confidentiality.

Performance

Performance is not a clear cut disadvantage of cloud computing although there are enabling features that increases the possibilities of having deficiencies in performance. The first feature is the distance from which between the infrastructure and the consumer. In addition, failure of selecting a reliable service provider may lead to deteriorating performance with time when more tenants are there sharing the same infrastructure (Sadiku, et al., 2014).

Reliability

A worst reliability is another drawback that is a result of the loss of control and performance issues. Reliability also is dependent on the cloud service provider. Cloud service providers vary in managing performance, availability and control issues. All of which affects the reliability level of the service.

Bandwidth Cost

When cloud computing came into the picture bandwidth was a very important and significant factor that questions the feasibility of cloud computing. Nowadays this issue is more relaxed since extra-large bandwidth networks are in place in different scales. Having that said, bandwidth cost is still an issue that depends on two factors.

The first factor is the intense of the data being transferred over the communication channel. The data intensity depends on the application and the type and amount of processes thin clients in the consumer sides does (Bhisikar & Sahu, 2013).

The second factor is the type of channel required that is dependent on the confidentiality and reliability level. A consumer that requires a dedicated communication channel that is not part of a public internet or public service providers will have to pay more for that dedicated bandwidth. In addition, dedicated TCP/IP bandwidth is different from dedicated traffic that is transferred on different protocol that is more reliable (Bhisikar & Sahu, 2013).

Security

It is quite interesting that security is listed in the advantage and the disadvantages sections and that is because of the wide range of aspects and varied domain that is considered to be the cyber security domain. It is beneficial to mention that if the security disadvantages are dealt with appropriate actions and remediation.

It is very much clear that all of the issues whether an advantage or a drawback depends on how service providers deal with it and act upon (Bhardwaj & Kumar, 2011). The process of choosing the service provider is very important and doing that carefully and according to international and national standards is a recommendation in this thesis that is also highlighted in chapter six, conclusions and recommendations: storage optimum security proposal.

3.4 Cloud Architecture and Infrastructure

The architecture of cloud computing is defined based on three major terms that is explained in this chapter as shown in figure (13). These three terms are characteristics, service models and deployment.

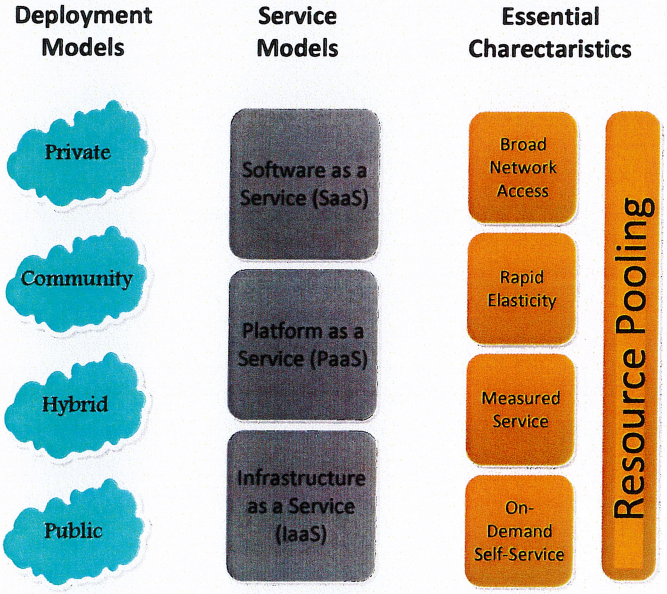


Figure (13)
Cloud Definition Components

In order to achieve the characteristics of cloud computing, virtualization as a concept is utilized. A data center with large capacity hardware is used over which virtualization is deployed to construct IaaS environment (Bhisikar & Sahu, 2013). Virtualization aggregates the resources of hardware available and utilizes them in the deployments

requested or built up. Using the IaaS environment, all types of different services of different scales are provided to consumers (Bilski, 2007).

Virtualization is an enabling technology for cloud deployments. Virtualization has been used by many IT professionals for installations and in-house deployments before cloud computing. Virtualization abstracts the hardware and enables creation of virtual machines managed by a virtualization management layer called hypervisor as shown in figure (14). This arrangement allows cloud services to be scalable and multitenant (Leavitt, 2009).

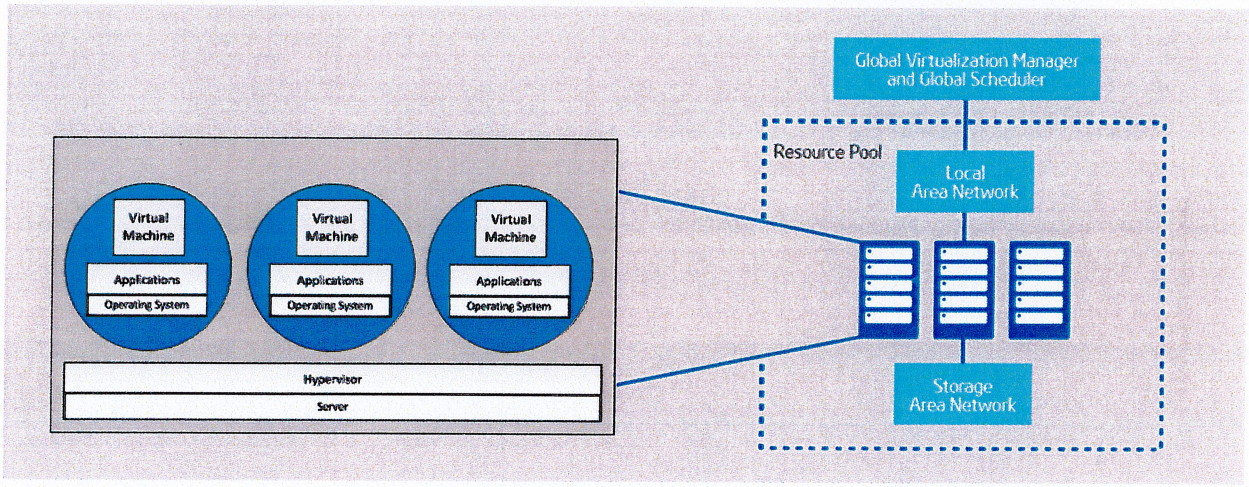


Figure (14)
Cloud Virtualized Architecture

3.5 Challenges and Future of Cloud Computing

Organizations and companies tends to concentrate on the core business they perform and that is why they have a habit of subcontracting any service that is not in the core business specially if subcontracting the job do not affect the performance and the efficiency and the cost as well (Bhardwaj & Kumar, 2011).

A lot of the work related to IT stuff has been subcontracted from a very long time but always the subcontractor mobilizes to the organization perimeter and work on their system (Bhardwaj & Kumar, 2011). When

cloud services came into the picture the domain of subcontracting has been widened and the whole service and infrastructure has been subjected to subcontracting (Mell & Grance, 2011).

Many organizations were reluctant to do so at the beginning similar to any new technology and specially the performance, efficiency and security were all topics that is still does not give a strong confidence for a transition to cloud. In the latest years and as the technology enhances and introduced positively in front of the public and private sector, several companies has at least migrated some of its services to the cloud. At the same time, a lot of critical industries and confidential organizations have not taken such a step (Riedel, et al., 2002).

It is very obvious for the principal researcher in this thesis and after going through a tremendous number of literatures that most of the questions and doubts have answers and different options are available for different categories of organizations within the domain of cloud services technologies.

Chapter 4: Storage System Cyber Security Assessment Case Study

4.1 Assessment Plan for the Local Storage System

4.1.1 Quantitative and Qualitative Assessment

4.1.2 Targeted Domains of the Assessment

4.1.3 Risk Matrix

4.1.4 Local Storage System Assessment

4.2 Pre-Assessment Questionnaire for Storage Systems Custodians

4.3 Storage Security Domains, Criterions, and Weighing Questionnaire for Cyber security Systems Custodians

4.3.1 Application Access Security Domain

4.3.2 Management Access Security Domain

4.3.3 Backup, Replication and Archive Security Domain

4.4 Supporting Questionnaire for discussion and conclusions

4.5 Assessment of Local Storage Systems of Organization "Alpha"

4.5.1Assessment Results

4.5.2 Discussion and Conclusions

4.6 Assessment of Local Storage Systems of Organization "Beta"

4.7 Techniques for Improving Security of Local Storage Systems

Chapter 4: Storage System Cyber Security Assessment Case Study

The first assessment conducted in this thesis is for an organization that is using local storage systems and is not relying on cloud services for storage systems. In order to do the assessment, a plan is prepared based on which the assessment questionnaire and interviews are prepared and the analysis of the feedback is done.

4.1 Assessment Plan for the Local Storage System

Assessment specialists identify major and essentials definitions based on which the assessment is conducted. These bases of assessments are discussed in the following sections.

4.1.1 Quantitative and Qualitative Assessment

The first definition is the qualitative or quantitative base of the assessment. In order to conduct an assessment of any type the practitioner of the assessment needs to choose either to do a quantitative assessment or qualitative assessment. A quantitative assessment is used when a money value can be assigned to risks or vulnerabilities and breaches in the cyber security case of our study. Quantitative assessment is an exercise of quantification (Gnanasundaram & Shrivastava, 2012).

A qualitative assessment in comparison is an assessment of a quality major rather than quantity (Elva, 2012). The assessment results are categories that are defined based on experts studies, research and literature. The assessments that is conducted in this thesis are qualitative assessments due to the fact that quantifying the impact of cyber security breaches is a huge exercise that requires dedication from a lot of personnel from the organization under assessment because the value of information and the value impact of a security breach is not a straight

forward number that is available in the organization. Qualitative values of the impacts in this research are based on literature and research available on Storage systems.

4.1.2 Targeted Domains of the Assessment

The assessment is applied on a certain system which is in this thesis the storage system. The cyber security of storage system is a big domain that is difficult to assess if taken as a single identity. An organization can be strong in one domain of cyber security such as the administration aspect that is for example covered by strict procedures and technology controls but at the same time weak from infrastructure security point of view with regards always to storage system (Alexander & Cowley, 2010). For this reason, Storage security domains have been introduced in chapter two and defined to be application access, management access and backup, replication and archive domains. For the sake of the assessment, the storage security domains are further classified and divided into more specialized domains to be assessed.

4.1.3 Risk Matrix

For the assessment plan a risk matrix have been identified and utilized for the risk ratings based on the impact and probability. Note that, impact and probability are also referred to as consequence and likelihood in literature. The general trend of risk matrices follows the theorem which states that the risk increases when any one of the two arms consequence and likelihood increase. The following is a risk matrix that is based risk matrix philosophy explained earlier (Alexander & Cowley, 2010). This matrix as shown in figure (15) presents an equal distribution of risk categories.

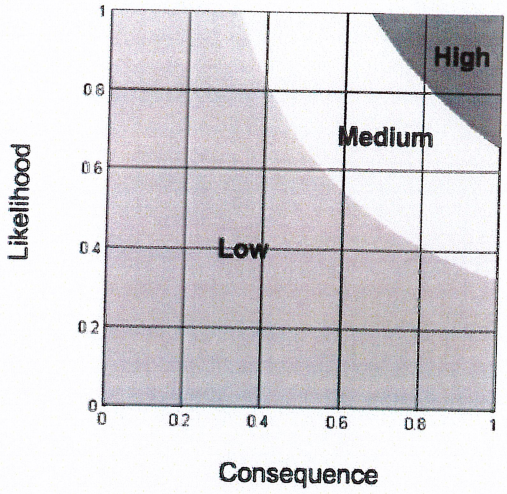


Figure (15)
Equal distribution risk matrix (Alexander & Cowley, 2010)

The model suggested in (Alexander & Cowley, 2010) is a general model that is found to be followed in most of the scientific assessments that have assessed the risks. The following figure (16) is another representation of the same model by the public safety Canadian authorities (Public Safety Canada, 2011).

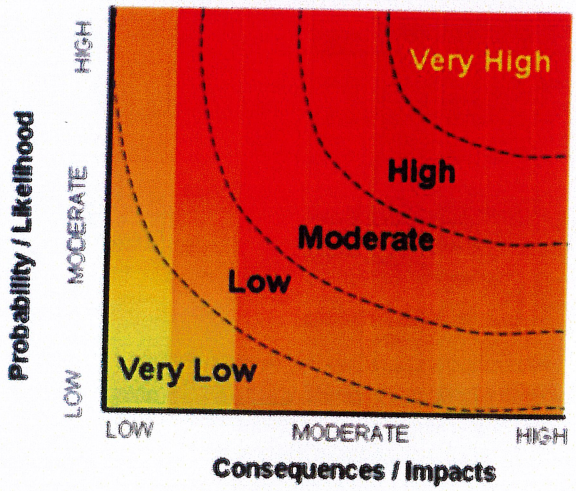


Figure (16)
Heat Diagram of Canadian public safety risk matrix (Public Safety Canada, 2011)

In literature, a number of different matrices are used that differs in size. Some uses (3 by 3) matrices and some goes up to (5 by 5) or (7 by 7). In this thesis, a (3 by 3) matrix is utilized in order to make it simple.

The (3 by 3) risk matrix utilized, figure (17), follows the same trend of risk matrices and specifically results in low risk for low impact or low probability is determined. High risk when both impact and probability are high and moderate risk for the rest of the cases as visualized in the following figure.

Risk Matrix		Impact		
		Minor	Moderate	Major
Probability	Likely	Low	Moderate	High
	Moderate	Low	Moderate	Moderate
	Unlikely	Low	Low	Low

Figure (17)
3 by 3 Risk matrix utilized in this thesis

(Eight to Late, 2009) and (Elva, 2012) are examples of literature that have utilized an exact similar matrix in its research for industries, projects and banks risk management respectively.

4.1.4 Local Storage System Assessment

In this assessment and as stated earlier the storage security domain is classified into the following domains (Gnanasundaram & Shrivastava, 2012).

1. Application access domain.
2. Management access domain.
3. Backup, replication and archive domain. As shown in figure 2-8.

These domains are assessed based on a number of criteria for each domain. Each criterion is assessed based on two measures (Alexander & Cowley, 2010). The first one is the impact which is categorized into:

- Minor

- Moderate
- Major

The impact of the criterion is resulted from its significance and possible risks it imposes on storage systems. The second measure is the probability of being compromised which is also categorized to:

- Unlikely
- Moderate
- Likely

In order to know the probability of the security failure or the occurrence of certain criterion, questions are asked for custodians of cyber security of storage systems based on which the probability is determined. In other words, the number of questions that is answered negatively determines whether the risk criterion is Unlikely, Moderate or Likely.

The probability assignment process is ended up with unlikely result if the number of questions that are answered negatively is less than one third of the questions asked in a certain criterion. Similarly, if the negative answers are between one third and two thirds of the total question, the probability ends up being Moderate and if the negative answers are more than two thirds the probability ends up being likely.

Based on the impact and probability, the risk is identified using a 3 dimension risk matrix as high, medium and low as per Figure (17). Figure (18) is an overall diagram that shows the sequential processes of the risk assessment.

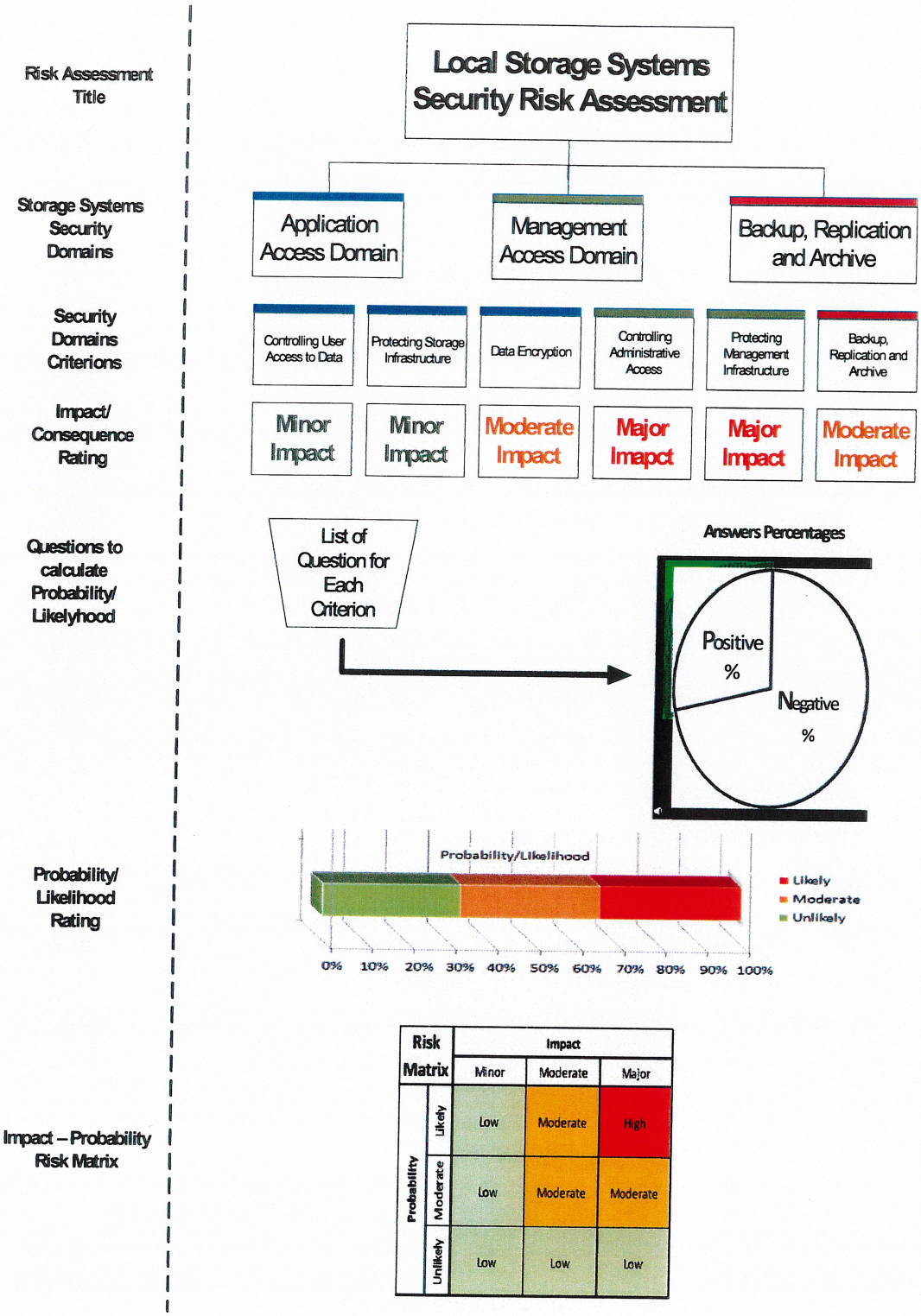


Figure (18)
Overall sequential processes of the Security Risk Assessment

4.2 Pre-Assessment Questionnaire for Storage Systems Custodians

In the pre-assessment questionnaire the questions are related to storage systems in general. The questions are listed in appendix A.

4.3 Storage Security Domains, Criterions, and Weighing Questionnaire for Cyber security Systems Custodians

In this section, the storage security domains and their criterions are listed. In addition, the impact of each criterion is declared along with the questions that are designed for storage system cyber security custodians to determine the probability of occurrence of each criterion.

4.3.1 Application Access Security Domain

This domain and as explained In chapter two, includes accessing data through applications such as database clients or file systems or any other method of data access. The criterions along with the questions associated to it are listed in appendix-A.

4.3.2 Management Access Security Domain

Management access domain includes all types of management access such as monitoring and configuring devices that are related to the storage system infrastructure (Gnanasundaram & Shrivastava, 2012). The criterions along with the questions associated to it are listed in appendix-A.

4.3.3 Backup, Replication and Archive Security Domain

Backups are of high importance to be considered as a separate security domains especially for entities that considers data confidentiality

to be of high importance. This domain will be considered as one criterion only in the assessment (Gnanasundaram & Shrivastava, 2012).The criterion along with the questions associated to it are listed in appendix-A.

4.4 Supporting Questionnaire for discussion and conclusions

Supporting questions for discussion are listed in appendix-A.

4.5 Assessment of Local Storage Systems of Organization "Alpha"

Organizations names are hidden in this thesis because of the sensitivity of information that is related to the cyber security of their systems. Names of the interviewed personnel are hidden also due to the same reason.

The first organization under assessment is referred to as "Alpha" in the rest of the thesis for simplicity. Similarly the second organization under assessment is referred to as "Beta" for simplicity as well. An interview has been conducted with the storage systems and Cyber security systems custodians in the organization "Alpha" on 12th of March 2014.

The person interviewed was the network specialist of the organization. The network specialist has had his bachelor degree in business Information systems in 2009. He has more than five years of experience in the field of IT systems. He has a wide range of certificates in the fields of project management, Microsoft systems, auditing, networks and network security.

In this interview the questionnaire has been answered and the storage systems cyber security has been discussed thoroughly. The detailed answers of the questionnaire that has gone through couple of review cycles with the Organization "Alpha" IT department are appended to this thesis in appendix B. In the following the assessment plan is applied on the questionnaire results and the results is discussed along with the conclusions of the situation of local storage system cyber security of organization "Alpha".

4.5.1 Assessment Results

Organization "Alpha" has four Storage systems. Two of which are SAN systems, one is NAS system and the fourth is a tape drive. The SAN systems are used for servers and applications data storage. One of the SAN systems is a DELL system has a capacity of 15TB. The other SAN system is an IBM system that has a capacity of 10TB.

The NAS system is also a DELL system that has a capacity of 25TB and is used for backup and restores purposes. The last system is HP system tape drive that is used to create long term onsite and offsite backup tapes.

All of the systems are windows based and are being used on a daily basis with a total maximum flow rate of 100 Giga Byte.

In order to have a basic understanding of the systems management aspect of the storage systems, introductory questions have been asked to the administrators and it has been realized that organization "Alpha" have service level agreements and licensing agreements that covers some of the managing aspects of the storage systems as well as other IT systems. It is also realized that there are no dedicated personnel looking after storage server's neither only nor dedicated personnel for cyber security

only. The person who is responsible for networks is also responsible for cyber security.

It has been realized also that organization "Alpha" is planning to have a cloud platform hosted by a cloud service provider for a wide range of services including some of the storage services. These services include but not limited to applications, file server, workflows, website, and collaboration tools. The questionnaire that is based on the assessment plan has been answered by organization "Alpha" and the assessment plan has been applied. The results of the assessment plan for organization "Alpha" are summarized in Table (1).

Table (1)
Assessment Results of Organization "Alpha" Storage Systems Cyber security

	Criterion	Impact	# of Questions	Not Applicable	Positive	Negative	Probability Calculation	Probability	Risk
Application Access Security Domain	*Controlling User Access to data*	Minor	11	0	9	2	0.181818182	Unlikely	Low
	Protecting the Storage Infrastructure	Minor	9	1	4	4	0.5	Moderate	Low
	Data Encryption	Moderate	6	0	1	5	0.833333333	Likely	Moderate
Management Access Security Domain	*Controlling Administrative Access*	Major	9	0	4	5	0.555555556	Moderate	Moderate
	Protecting the Management Infrastructure	Major	8	0	5	3	0.375	Moderate	Moderate
Backup, Replication and Archive Security Domain	*Backup, Replication and Archive Security Domain*	Moderate	7	0	0	7	1	Likely	Moderate

Most of the risks are found to be Moderate and they are in the high moderate that is close to be High risk. Only two risks are found to be Low and they are low just because their impact on system is Low but the probability that is based on cyber security performance is still high in being breached. The drawbacks that have led to this severe situation are listed in this chapter.

The first criterion "Controlling User Access to Data" is in the application access security domain. This criterion has a minor impact on

cyber security as a whole since compromising it is equivalent to having an unauthorized host or user that has in nature limited privileges that cannot impacts the systems and data widely.

Questions assessing the probability of compromising this criterion were eleven, nine of which has been answered positively and two of which has been answered negatively. The positive measures were having centralized technical controls for hosts authentication and authorization, having administrative procedure and account management documents that controls authorization and authentication, having access control lists on storage systems for users, having regular auditing over technical and administrative controls of authorizations and authentication, and having security logging that is secured from hosts' access.

The only two negative points in this criterion for organization "Alpha" is the lack of virtual LANs that restricts users' access and the lack of a centralized continuously monitored security center for monitoring, prioritizing and communicating logs.

The risk of the first criterion has ended up being Low as a result of a Minor impact and unlikely probability according to the risk matrix. The second criterion that is also in the Application Access security domain and has minor impact is "Protecting the Storage Infrastructure".

Questions assessing the probability of compromising this criterion were nine, four of which has been answered positively and four of which has been answered negatively and the a question that is related to wireless access to storage system is not applicable. The positive measures were having physical security on the storage infrastructure, having security controls from unauthorized network connection that reports also unauthorized access attempts, and having a separation of duties procedure.

The four negative points in this criterion for organization "Alpha" is the lack of centralized monitored security center, the utilization of unencrypted protocols on the storage network, the lack of RBAC and having the management and users traffic on one network. Although the probability of compromising this criterion is Moderate, but because of the Minor impact of the users storage infrastructure, the Risk is ended up being Low.

The last criterion in the application access security domain is "Data Encryption". This criterion unlike the previous two have a Moderate impact on cyber security as a whole since compromising it is equivalent to thieving data media or tampering with data that may compromise the whole confidentiality and integrity. Questions assessing the probability of compromising this criterion were six, one of which has been answered positively and the rest has been answered negatively.

The only positive measure is having physical security over the storage infrastructure. The rest negative points in this criterion for organization "Alpha" are the lack of data encryption on the storage system and in transit between end users and storage systems, the lack of write off procedure for storage media that reaches end of life, and the lack of antivirus and other integrity insurance software on storage systems.

The risk of this criterion is moderate resulting from the Moderate impact that it has and the likely probability of being compromised as per the risk matrix. Management access has two major impact criterions. Compromising any of these two criterions is equivalent in a way or another to having an unauthorized management access that can affect confidentiality, integrity, availability and accountability as well. The first is "Controlling Administrative Access" criterion.

Questions assessing the probability of compromising this criterion are nine, four of which are answered positively and five of which are

answered negatively. The positive measures are having access control on storage systems, having strong third party centralized server for authentication, having RBAC on management ports and having a strong security level on logs.

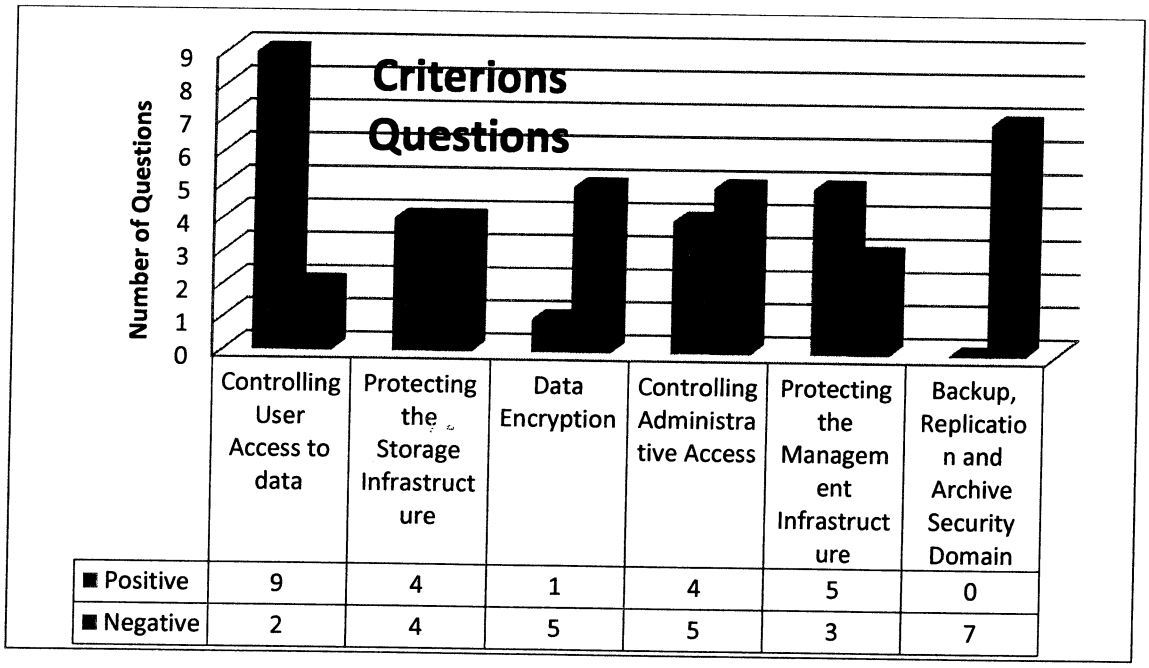
The five negative points in this criterion are the lack of power users with different roles which results into doing all administrative tasks using administrator account, the lack of centralized security center for logs which results in the inability of prioritization of administrative logs and the lack of centralized time server that results in weakness in following sequence of events in case of incidents.

The risk of this high impact criterion is Moderate because the probability is Moderate also as per the Risk Matrix. The second criterion is "Protecting the Management Infrastructure" criterion. Questions assessing the probability of compromising this criterion are eight, five of which are answered positively and the rest are answered negatively. The positive measures are having different levels of access control for management traffic flow, having in packet inspection devices as well as other network protection devices such as firewalls to protect the overall management traffic, restricting the number of hosts that have management access.

The three negative points in this criterion are the lack encryption for management traffic, the lack of a separate segment for management traffic and the lack of regular activities for blocking unused ports over the network. The three negative answers have pushed the probability of being compromised level to Moderate and consequently the risk also to Moderate according to the risk matrix.

The last but not least in impact security domain is the "backup, replication and archive security domain" which is a single criterion domain with Moderate impact affecting confidentiality and recovery

plans mainly and seven questions that assesses the probability of being compromised. All questions are answered negatively reflecting lack of remote disaster recovery site, lack of encryption in the backup creation process, unavailability of procedure for tape handling, lack of authentication in restoring backups, and the lack of regular validation tests for restoration process of storage systems. Figure (19) shows a statistical diagram showing the positive and negative answers amount for each and every domain.



	Controlling User Access to data	Protecting the Storage Infrastructure	Data Encryption	Controlling Administrative Access	Protecting the Management Infrastructure	Backup, Replication and Archive Security Domain
Positive	9	4	1	4	5	0
Negative	2	4	5	5	3	7

Figure (19)
Criterion Questions Results for "Alpha"

All of these results and the answers of supporting questions that are not part of the assessment are discussed in the following section.

4.5.2 Discussion and Conclusions

Before starting discussing the assessment, the fact that there is no dedicated personnel for storage systems nor for cyber security that is figured out from the preliminary questions that have been asked to the storage systems custodians gives a bad indication that allow to understand and expect negative results in the assessment.

The results of the assessment show four Moderate risks of four criterions and two Low risks for the rest two criterions. In addition, the probability of being compromised in two of the criterions which are the backup and the data encryption criterions have been very high (likely) although it resulted in a Moderate risk due to the Moderate impact it has. Figure (20) shows the overall risk rating percentages of this organization.

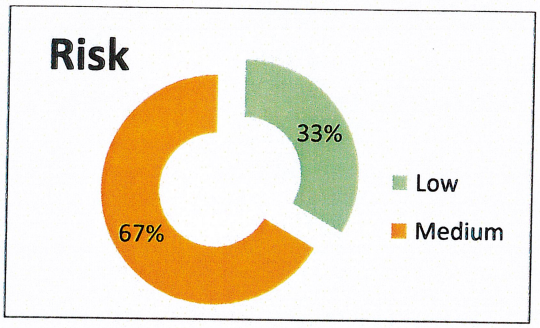


Figure (20)
Risk rating percentages for "Alpha"

Details of probabilities and impacts that have led to the risk rating results are illustrated in Table (2).

Table (2)
Risk Matrix Results of "Alpha"

Risk Matrix		Impact		
		Minor	Moderate	Major
Probability	Likely	Low	Moderate (2)	High
	Moderate	Low (1)	Moderate	Moderate (2)
	Unlikely	Low (1)	Low	Low

In addition, the answers of the question related to protecting the storage infrastructure from an application access point of view are not very pleasant and resulted into a Moderate probability of being

compromised but is not reflected in the risk results because of the low risk suggested for that criterion.

Having all of this said, the impact suggested is based on relational impact analysis but are not always true and may vary depending on the organization and the other factors. The exercise of having exact impact figures have not been done in this thesis because of the complex and gigantic amount of efforts such exercise may take.

The following is a summary of the weak aspects of the cyber security framework of storage systems in organization "Alpha", the weak aspects are taken from the assessment questionnaire and the supporting questions answered by organization "Alpha". These drawbacks have led to the results that show organization "Alpha" as an organization with many standing risks in terms of cyber security.

1. There are no dedicated personnel for storage systems or for cyber security.
2. There are no virtual LANs on the network that segregates different types of traffic and access privileges.
3. There is no centralized continuously monitored security logging system that aggregates all of the different security logs from the storage infrastructure devices.
4. There is no encryption on storage systems or in transit over the different components of the storage infrastructure.
5. There is no Role Based Access Control.
6. There is no write off procedure for storage media.
7. There is no antivirus software on the storage system or integrity insurance software.

8. There are no power users that have different levels of administrative tasks and privileges and the Administrator account with full privileges is used for any kind of administrative task.
9. There is no centralized time server for all of the components of the storage infrastructure.
10. The management traffic is not encrypted.
11. The management traffic in on the same network as the data traffic.
12. The ports on the network are not checked regularly to block unused ports.
13. There is no remote disaster recovery site.
14. The backups are not encrypted ad have no authentication requirement for restoration.
15. There is no procedure for backup tapes handling.
16. The backups are not tested by having regular restoration procedure.
17. The governing part of cyber security is handled by the same entity responsible for the implementation of it.
18. The organization does not benchmark its cyber security framework against comparatives.
19. There is no disaster recovery plan or business continuity management procedure.
20. There is no obselesance management procedure.
21. There is no data retention policy and procedure.

In conclusion, the cyber security of storage system in such organization is not as it should be. Although this has not resulted in a serious failure but issues may appear at any point of time due to the high number of vulnerabilities as reflected in the assessment results.

4.6 Assessment of Local Storage Systems of Organization "Beta"

Another important organization in the public sector has been gone through the assessment in order to confirm the results which we have reached in the first assessment. Representatives from organization "Beta" IT department have been interviewed on 12^{h} of March 2014 in which cyber security of storage systems have been discussed.

This IT representative holds the position of senior infrastructure and network administrator in the organization. He has got his bachelor degree in engineering informatics in 2009 followed by a master degree in computer science in 2012. He has gone through five years of experience in the field of IT systems. He has wide range of certificates in IT systems such as Cisco Certified Network Associate (CCNA) in networks, Microsoft certified Solutions Associate (MCSA) in Microsoft solutions and Symantec backup Exec (SBE) in Symantec backup and recovery solutions

The detailed answers of the questionnaire that has gone through couple of review cycles with the organization "Beta" IT department are appended to this thesis in appendix C. From the introductory questionnaire, it is realized that the storage systems status and configuration are almost the same with organization "Alpha". organization "Beta" also has three types of storage systems SAN, NAS and tape drive for the same purposes. The NAS and SAN is Fujitsu this time and tape drive is also HP system. The operating system for organization "Beta" storage is Linux kernel.

Organization "Beta" has also no dedicated for neither the Storage systems nor the cyber security. In contradiction with organization "Alpha", organization "Beta" has no plan and is not interested in going to

cloud because they are concerned of the confidentiality of the data they have.

The questionnaire that is based on the assessment plan has been answered by organization "Beta" and the assessment plan has been applied. The results of the assessment plan are summarized in the table (3).

Table (3)
Assessment Results of Organization "Beta" Storage Systems Cyber security

	Criterion	Impact	# of Questions	Not Applicable	Positive	Negative	Probability Calculation	Probability	Risk
Application Access Security Domain	*Controlling User Access to data*	Minor	11	0	9	2	0.181818182	Unlikely	Low
	Protecting the Storage Infrastructure	Minor	9	1	5	3	0.375	Moderate	Low
	Data Encryption	Moderate	6	0	2	4	0.666666667	Likely	
Management Access Security Domain	*Controlling Administrative Access*	Major	9	0	4	5	0.555555556	Moderate	
	Protecting the Management Infrastructure	Major	8	0	5	3	0.375	Moderate	
Backup, Replication and Archive Security Domain	*Backup, Replication and Archive Security Domain*	Moderate	7	0	4	3	0.428571429	Moderate	

As the case of organization "Alpha", most of the risks in organization "Beta" are found to be Moderate and they are in the high moderate that is close to be High risk. Only two risks are found to be Low and they are low just because their impact on system is Low but the probability that is based on cyber security performance is still high in being breached.

Figure (21) shows a statistical diagram showing the positive and negative answers amount for each and every domain.

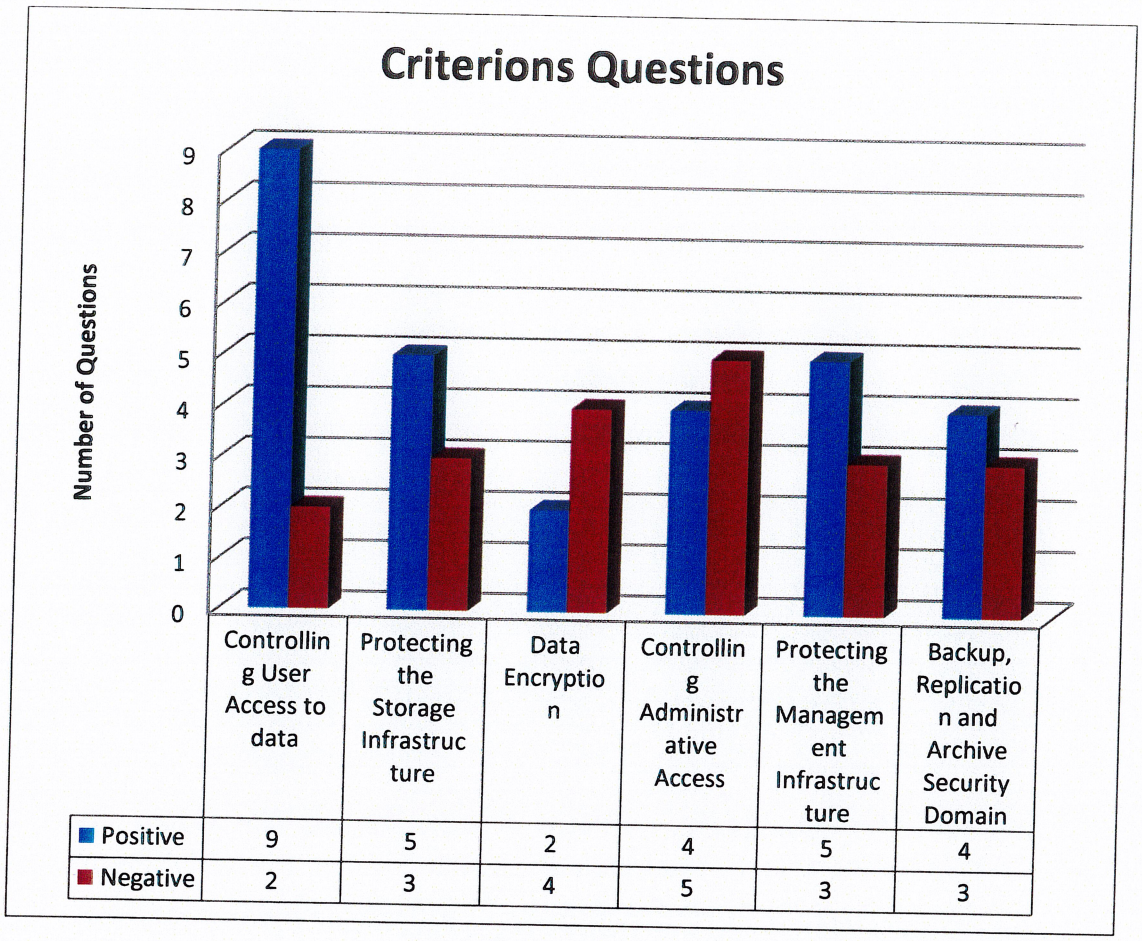


Figure (21)
Criterion Questions Results of "Beta"

The assessment results are remarkably exactly the same as the organization "Alpha". Results from the final risks ratings aspect although the two organizations are independent, the answers to the questions are different and aspects into which organization "Alpha "is weak are different from aspects in which organization "Beta" is weak in many cases. The overall risk rating percentages for this organization is as shown in figure (22).

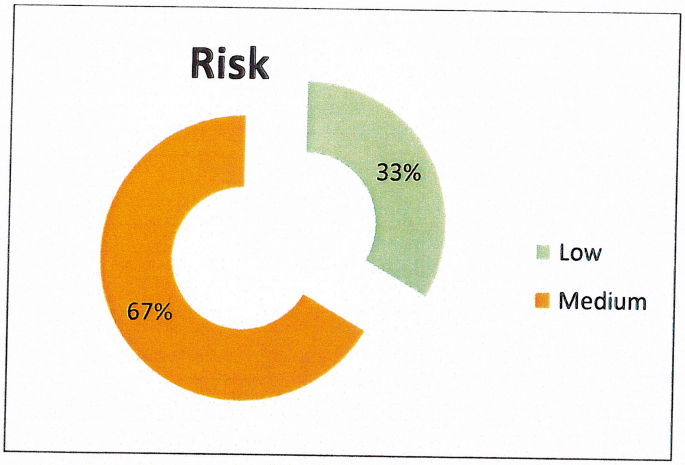


Figure (22)
Risk Rating Percentages for "Beta"

The results of the assessment show four Moderate risks and two Low risks. In the assessment and in contrast to organization "Alpha" assessment, the results is better form probability point of view and the only criterion into which the probability of being compromised is likely is the data encryption criterion which has Moderate impact the resulted into a Moderate risk according to the risk matrix. Details of the probability and impact results yielded to which square in the risk matrix is in Table (4).

Table (4)
Risk Matrix results of "Beta"

Risk Matrix		Impact		
		Minor	Moderate	Major
Probability	Likely	Low	Moderate (1)	High
	Moderate	Low (1)	Moderate (1)	Moderate (2)
	Unlikely	Low (1)	Low	Low

The results confirms the conclusion of the existence of weaknesses and vulnerabilities in local storage systems cyber security specifically when there is no dedicated staff to look after cyber security and storage systems which is the case in many organizations.

The weaknesses in organization "Beta" in addition to the lack of dedicated staff are summarized in the following points resulting from the assessment questionnaire and the supporting questions as well:

1. The lack of auditing over administrative and technical controls for Users/Hosts authentication and authorization.
2. There is no encryption mechanism in place for data neither on storage system nor on transit.
3. There is no role based access control RBAC implemented on the storage system.
4. Management network is not separated from users' data network.
5. There is neither antivirus engine nor data integrity software on the storage system.
6. There are no power users that have limited privileges for specific administrative tasks.
7. There is no regular activity for disabling unused network ports on the storage systems infrastructure.
8. Backup solution in use does not encrypt data backed up.
9. There is no procedure that is followed for tapes handling.
10. There is no regular restoration/validation procedure for backups.
11. The governing part of cyber security is handled by the same entity as the implementation part.
12. The infrastructure resources available for hosting the storage services are not sufficient.
13. There is no resources for continues security logs monitoring.

14. There are no scheduled plans for penetration tests for storage systems infrastructure.
15. There are no benchmarking activities against similar organization's security framework.
16. There is obselesance management plan.

An abstract comparison between the two assessed organizations in terms of overall positively and negatively answered questions is shown in figure (23).

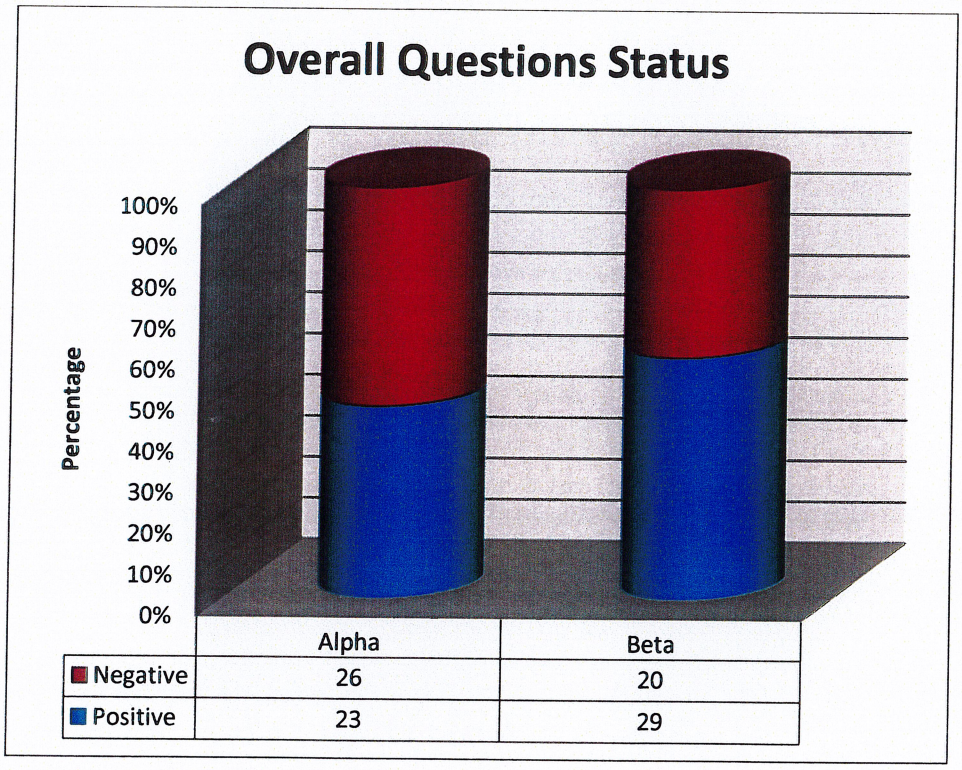


Figure (23)
Overall Questions status of the two organizations assessed

4.7 Techniques for Improving Security of Local Storage Systems

Regardless the transition to cloud proposal which is recommended in this thesis, organizations with local storage systems can improve the cyber security of their storage systems by applying certain techniques that may cost the organization more and add more processing load on the

available infrastructure that may need upgrades to remove some issues with may affect the performance.

The following are some of the techniques that improve the cyber security of storage systems specifically in the organizations that has been assessed in this thesis. These techniques are suggested based on the negative points that have been raised in the assessment result

Staff Dedication and Security Awareness

Staff dedication is one of the most important factors in cyber security nowadays (Gupta & Kaur, 2013). This aspect is missed and is not given the correct attention in most of the organizations. The reason is the freshness of the topic and the difficulty in reviewing organizational charts and the cost optimization processes.

Cyber security is currently a wide field that has many details which cannot be handled in the way it should be in the part time of IT personnel. In the legacy of IT organizational charts, the separation of systems, network and telecommunication, help desk and projects responsibilities are taken into consideration depending on the volume of systems of the organization (Gupta & Kaur, 2013). Cyber security unfortunately is not given the same attention.

In some organizations such as the organizations that have undertaken the assessment, the cyber security responsibilities is given to network professionals due to the relevant competency needed in managing firewalls and network infrastructure. Apparently, this was good enough couple of years ago but not now after the tremendous increase of security attacks and concerns in all of the different components of IT infrastructure starting from hardware level up to all of the different Software applications.

All above shows that training the IT employees, who manage all different aspects and functionalities of IT systems in information security, is very important and critical millstone for improving the cyber security of IT systems including storage system.

Dedication of employees for cyber security has another aspect as well that is the governing role of cyber security. In order to ensure cyber security in an organization, the elements of successful organization, people, process and technology applies also (Gupta & Kaur, 2013). Ensuring that the process side is safe and well maintained according to standards is an outcome of good policies and procedures system that is initiated and maintained by a cyber-security professional other than the personnel responsible for the implementation.

The lack of staff dedication is mentioned here and at the beginning of this section because it is the root cause of many other problems in the cyber security framework. The two assessments show lack of staff dedication as well as responsibilities splitting matrices (Gupta & Kaur, 2013).

RBAC (Role Based Access Control) and Network Segregations

Most of the current cyber security framework designs are based on the concept of defense in depth in which the idea of network zones and conduits is a base stone. Having a flat network that allows an intruder to go everywhere is a major vulnerability in computer networks. Network segregation is the solution.

Network segregation makes it difficult to access a segment from the network from another segment. An important example is segregation of management traffic network and data traffic network. The segregation will prevent a major compromise to happen, which is accessing all the management ports on the network, when a minor compromise happens,

which is accessing the data network that may be less secure or more probable since client access areas may not be in the same level of physical security of the data centers or management access (Gupta & Kaur, 2013).

A role based access control is also a very significant segregation mechanism and security technique that prevents an accountant from accessing the human resources network segment based on his role for example. Network segregation is another area of concern in organizations because it requires a lot of efforts to make a neat design that does not affect availability and processes and at the same time ensures the level of segregation that hardens the network security.

SIEM (Security Information and Event Manager)

IT systems nowadays have logging mechanisms by default and as an essential add-on. This applies to all of the components of the storage systems infrastructure such as switches, firewalls, Intrusion Detection and Prevention Systems (IDP), domain controllers, time servers, and storage systems themselves. Although all of the logs are always available and maybe secure access is also required to edit them, IT personnel does not have the time and resources for reviewing the logs and correlate them. Such exercise requires a tremendous amount of efforts. In addition, a compromise will not be dedicated at the right time.

The solution is a center that aggregates all of the logs using different communication protocols such as SNMP and Syslog (Gupta & Kaur, 2013). To prevent opening a new security hole by transferring the security logs of the network, this traffic is considered as a management traffic that should be communicated over the dedicated management network segment as mentioned in the network segregation security technique.

After aggregating the security logs, certain rules and correlations should be applied on the logs to save repetitive efforts that employee need to do to correlate and understand the logs and in order to enhance the decision making process in response to security attacks (Gupta & Kaur, 2013). Finally meaningful and clear messages are communicated to the right personnel responsible for acting upon the logs and the communication can be in the most effective way available such as text messages or emails if the personnel have an easy solution to receive and brows emails such as smart phones.

The technical and commercial name for the system that does all of the tasks explained here has different names depending on the manufacturer such as Security Logging Manager or Security Information and Event Manager (SIEM). Many organizations such as the entities assessed in this thesis do not have such a system and if so it is only programmed once and not well maintained. Eventually and since cyber security is a very dynamic domain configuration and correlation rules are always subject to change.

Encryption

Encryption is one of the oldest security techniques that introduce a secure in nature data that is secure and unpredictable even in the hands of an intruder or attacker. The evolution of encryption is progressing in the same pace of decryption techniques and encryption break methodologies (Behl, 2011). For this reason, dynamic encryption robust methodologies that does not affect availability and ensures integrity as well should be considered by organizations.

In the case of storage systems, to secure the data, encryption is not only required on the storage systems itself but also required for data in transit whether over WAN or LAN. In addition, encryption is required

also for backups especially backups that are vulnerable to be stolen because of the absence of a strict procedure for handling such as tape handling (Behl, 2011).

Systems are currently more integrated and interconnected, backup are also required and remote disaster recovery is also a must for many organizations. Encryption should be everywhere to ensure the cyber security of the data. Organization and as concluded from the assessments done does not have encryption everywhere and are lacking in a way or another in the encryption security technique.

Policies and Procedures

If a person assumes that security techniques and enhancing cyber security framework is always using security solutions and technologies, that person is totally wrong. There are two other factors in addition to technology that have the same importance if not more. Those are people that we have mentioned under the staff dedication title and process that is forced and defined by policies and procedures. Policies define the laws for cyber security and procedures define how policies are implemented. A security framework cannot be effective although it has all of the state of the art technologies without policies and procedures for their management (Gupta & Kaur, 2013).

Policies and procedures are required to define responsibilities, set rules for allowed and not allowed usage, set frequencies and methodologies for updates and backups and several other tasks and duties (Behl, 2011). It is found in research that many organizations invest in systems that become ineffective after some time because of the absence of policies and procedures. In the assessment it is found also that some processes have no procedure and that may risk the continuity and sustainability of that process such as backup tapes handling management.

Administrative Tasks Management

As the risk assessment suggested, management security domain impact is high with respect to the other domains. This is true because a high level of authorization and access control exists on management network. In order to minimize that risk the full privilege Administrator access should not be used unless it is really required to have that level of access which is not the case for most of the administrative tasks.

A fact that should be in mind of systems administrators is that a virus or a malware on the system have the same level of access as you have or you are logged into. To implement and enforce this security technique and behavior, power users should be created with task tailored access privilege that allows executing certain domain of tasks (Gupta & Kaur, 2013).

An example is backup tasks, if a virus for instance exists on the backup server and requires authorization level that has the right to create shared folders in order to spread. If the administrator uses full privileged Administrator user to execute backups, the virus will take that opportunity and create shared folders (Gupta & Kaur, 2013). Otherwise, if the backup's creation power user is always used to create backups the virus will remain silent and be caught by the antivirus after a certain update which has its definition is installed.

In addition to the creation and usage of power users, distributing responsibility by assigning different power users to different personnel in the organization distributes powers and make it difficult to have a weak point in which all the authorities aggregates. Weak may mean an ignorant employee for instance.

In several organizations, either because of the amount of manpower exists or due to the fact that it is just easy and straight forward to use an administrator for all the tasks without thinking of what privilege is

needed, the administrator account is always used by IT administrators as it was highlighted by the answers in the assessments conducted. Listing all of the security techniques is never possible and each and every cyber security technique needs books and books by its own. Weaknesses found in the assessed organizations also have more security techniques required to solve them but for the sake of keeping pace and sticking to the scope and the goal of the thesis few security techniques have been mentioned which can be of a major enhancement for the cyber security framework of the assessed organizations.

The security techniques in discussion have many implications other than hardening the cyber security framework. The other implications are the cost value of the implementation and the organizational inflation that may happen. For this reason other solution exists and cloud is pioneer solution and attractive cost to avoid such implications that cannot be avoided if the cyber security is to be hardened.

Chapter 5: Cyber Security of Cloud Storage Services and Proposed Solution

5.1 Legacy Storage Systems and Cyber security Issues

5.2 Cloud Computing for Storage Services

5.3 Migrating Storage to Cloud

5.4 Cyber security of Storage on Cloud

5.4.1 Benefits for Inherited Issues

5.4.2 Introduced Issues

5.5 Storage Enhanced Security Recommendations

5.5.1 Organizational Steps for optimum security of storage systems

5.5.2 Cloud Migration Proposal

5.5.3 Mitigations against introduced cyber security threats of cloud computing

Chapter 5: Cyber Security of Cloud Storage Services and Proposed Solution

The opportunity of starting a new chapter is always utilized to recapture the idea of the research in this thesis and how the chapter content correlates to it. Assessing cyber security for storage systems when local installations is utilized and how it differs when a migration to cloud happens. The thesis ends up by proposing an approach for organization "Alpha" and organization "Beta" to follow and highlight recommendations and conclusions.

In this chapter and after introducing cloud computing in the previous chapter, the utilization of cloud for storage of organization "Alpha" and organization "Beta" specifically is discussed and the cyber security aspects of such utilization is discussed as well.

The chapter starts with a brief summary of local storage systems and their cyber security issues discussed in the introductory chapters. How storage services utilizes cloud capabilities and how such services are provided to consumers follows. After that guidelines for our case studies are given to migrate to cloud storage services in the optimum no losses scheme is highlighted.

The chapter ends with the core part of it, which is the cyber security enhancements and drawback of migrating storage to cloud. Enhancements are mainly mitigations for cyber security issues that are currently facing storage systems. On the other hand, drawbacks are mainly introduced issues that have been always the most discussed disadvantages of migrating to cloud.

5.1 Legacy Storage Systems and Cyber security Issues

It has been found that local storage systems suffers from different issues that cannot keep data safe with the current threats and capabilities of potential hackers and attackers in the world. Having that said, other solution should be taken in consideration and on one of them utilizing cloud computing in a way that stress on its benefits and get rid of any compromise specially in the cyber security field (Behl, 2011).

5.2 Cloud Computing for Storage Services

As a service model, storage cloud is an Infrastructure-as-a-Service type of service that gives consumer organizations a sufficient level of scalability and flexibility. The scalability and flexibility are in using the virtualized environment for its storage requirements. IaaS is the foundational level for other models and services (Dawoud, et al., 2010).

Cloud service providers costs the consumer three main categories of payments for storage services. Pre-Operation charges that are fixed normally and kits value depends heavily on the requirements of the consumer that is negotiated in the service contract formation stage (Bhardwaj & Kumar, 2011).

The other two categories of payment are variables and dependent on the amount of storage capacity required and the bandwidth required. In most of the cases, the first requirement which is the storage capacity has different classes of payments that are dependent on the capacity. In other words, the cost of 1 Giga Byte GB when the whole requirement does not exceed 1 Tera Byte TB is different from the cost 1 GB when the total requirement exceeds one TB (Bensoussan & SingRu, 2011).

The second variable cost is the bandwidth cost and that has also different rates for upload and downloads in most of the cases. In addition, part of the IaaS package is computational resources. This computational resource allows consumer users to use data stored without the need for download or upload. Cloud storage services are very attractive and allows consumers to transfer a number of their applications that are storage centric such as email systems, communication tools, data sharing and backup and restore management (Kumar, et al., 2012).

5.3 Migrating Storage to Cloud

The benefits and feasibility of transferring storage to cloud that is summarized in the question "Why transferring to cloud?" is not a doubtful topic anymore. Instead, the topic that is doubtful and pops up many discussions nowadays is "How to migrate to cloud?" and "How to transfer services to cloud?"

There are different approaches to migrate storage services and data from local systems to cloud infrastructure. All are dependent on the service provider, amount of data and systems, and security. There are even nowadays software packages that are specialized in migrating from one cloud to another.

In general there are some guidelines that are always true in any migration plan for storage services.

1. A migration plan should be developed carefully along with service provider and experts from the consumer side. If required, third party consultants should be hired to represent the consumer (Sitaram & Manjunath, 2011).
2. In-house efforts should be made to catalog all storage requirements. Architecture drawings and systems inventories should be developed.

3. In conjunction with the previous activity of inventorying and information gathering, a structure for authorizations and responsibilities should be developed to utilize the permissions and authorization features provided by cloud service provider (Gupta & Kaur, 2013).
4. Next, the files upload or transfer activity should be planned. Planning this activity should take into account the availability of the services which may lead to the utilization of non-business hours. If there are no non-business hours, which are the case for a lot of different ranges of businesses, an online or on-process migration should be planned.
5. The migration plan should take into consideration securing the data during the transfer (Gupta & Kaur, 2013)..
6. After having the storage data on the cloud service provider facility, handing over responsibilities between the local storage systems and the cloud storage infrastructure should be planned.
7. The operation after the migration should be tested and have a pilot period to ensure safe, secure and optimum performance (Gupta & Kaur, 2013).
8. Remediation should be applied to any issue happens during the testing period. Excellent logging system is required to capture issues before affecting business (Gupta & Kaur, 2013).

5.4 Cyber security of Storage on Cloud

Although cloud services may be foreseen as a solution to enhance the cyber security paradigm of the IT services an organization has, because the cloud service provider is a dedicated entity whose only business is to manage data centers and provide different levels of cloud services, cloud presents tremendous number of cyber security risk that are

directly related to the use of cloud instead of having the services locally hosted (Behl, 2011).

A recent survey shows that more than 80% of IT professionals believe that the biggest challenge with regards to cloud computing is security. Another study shows that in an enterprise of 5000 employees, the cost of security labor and productivity has dropped by 41% equivalent to 49$ per employee per year (Behl, 2011).

In this section, cyber security benefits of transforming to cloud are discussed followed by the downsides from cyber security aspect of the transformation.

5.4.1 Benefits for Inherited Issues

As explained, most of the benefits that cloud provides in terms of cyber security is because cloud service providers' only business is providing cloud services by managing and maintaining data centers.

- **Staff Specialization:** Similar to any other proficiency, IT organization size depends on the amount of work and scale of responsibilities. When the manpower is big, specialization comes into picture because there is a potential that allows doing so (Gupta & Kaur, 2013).

  For example, when accountancy responsibilities are of high scale such as in banking institutes an accountant have a lot of different specialized tracks to work in. In comparison, in another organization one or two accountants may do everything related to this domain without having specialty into a specific track.

  Cloud computing providers for IT personnel are like banks for accountants, and security is one of the tracks that have a specialized staff that works only on cyber security full time. On the other hand, and as seen in the assessment other organizations have

IT personnel that does everything including security (Gupta & Kaur, 2013).

- **Resource Availability:** Although availability enhancement in migrating to cloud may be challenged with the fact that the resources will be available through a multistage communications means and the availability is affected by the availability of the communication mean, availability is enhanced by looking into the matter from different angle (Bensoussan & SingRu, 2011). Infrastructures of cloud providers have by design redundancy, recovery and protection capabilities that reduce the possibility of having downtime to a very small fraction of the probability of in-house systems. In addition, when the traffic is high and resources are being acquired by users in a very high scale in some occasions, cloud providers will have the resources means to withstand in such situations although it might cost the customer depends on the contract agreement terms and conditions. In similar cases and when in-house systems do not manage to absorb the demand, systems may fail (Maddineni & Ragi, 2011).
- **Backup and Recovery:** It is obvious from the assessment done on the governmental organizations in chapter four that they do lack in backup mechanisms especially in the availability of offsite emergency or data recovery center. Cloud service providers have very robust backup and recovery capabilities and these capabilities are due to the fact that cloud providers business is the service that they are providing and they cannot withstand a failure in the service (Behl, 2011).
- **Remote Users:** In organizations that have IT systems onboard and do not use cloud services, an employee who needs to access organizational data on the go either take a copy of the data on the

mobile device used or have a remote connection to the organization systems. Both methods are dangerous and impose security thread because a mobile device may be stolen and as explained remote access security measures wouldn't be robust (Behl, 2011). In cloud computing, consumer is always in a remote condition whether in the company premises or not and securing the communication channel is a business must and interest always (Bensoussan & SingRu, 2011).

Data Concentration: Because of the homogenous nature of systems structure in cloud data centers, a central storage system concentrates all of the data of a certain entity whereas in in-house based installation mostly data are scattered among systems and users (Maddineni & Ragi, 2011).

5.4.2 Introduced Issues

In this section, some popular and common security issues and drawbacks that are introduced from migrating to cloud are discussed.

- **Shared Multi-Tenant Environment:** In most of the cases the cloud services provider serves multiple consumers and the resources available for consumers are separated logically rather than having physical separation. Such logical separation poses cyber security threat but is part of the integral idea and philosophy of cloud computing (Dinadayalan, et al., 2014).

  An intruder may utilize the access given to him as a consumer and find out a way to overcome the logical boundaries available to attack certain entity that utilizes the same cloud service (Bensoussan & SingRu, 2011).

- **Public Networks exposed services:** Before having cloud services, all IT services were hosted internally in the organization and

protected by the physical means of organizational physical security (Maddineni & Ragi, 2011). Cloud services are hosted in a remote location from the organization and have a communication channel that communicates the services and data back and forth between the service provider and the consumer (Behl, 2011). The communication channel have a variety of fashions, some utilizes the internet which imposes very high risk due to the wide exposure surface. Others use telecommunication utilities infrastructures for dedicated communication channels. In some rare cases, consumer has a dedicated self-owned communication line all the way to the service provider.

Security is availability and Integrity as well and those factors may also deteriorate when a public communication channel is utilized (Bensoussan & SingRu, 2011).

The last but not least security drawback related to exposure to public networks is that in some cases and in addition to the data access, administrative access is also exposed as well.

- **Loss of Control:** Although cloud providers have highly specialized staff that may not be possible to mobilize by organization in-house, but the application of all security policies and procedures is under the control of cloud provider (Riedel, et al., 2002).

  This makes a lot of security aspects vague for the consumer organization such as compliance, incident response, accountability and everything that is affected by losing the direct control.

5.5 Storage Enhanced Security Recommendations

Organizations are recommended to consider the option of migrating storage services to cloud but with several precautions and advices that

should be followed strictly in order to avoid making a strategic mistake instead of making a strategic move to the future.

5.5.1 Organizational Steps for optimum security of storage systems

The research in this thesis is a very rich substance for an organization to have a clue of the way forward for their IT systems and cyber security resilience.

The following is a summary of conclusions and recommendations that is followed by an elaboration of the proposal of consideration. The cyber security assessment in chapter four has been conducted for two prestigious governmental organizations. It is believed that the results apply on a wide spectrum of governmental, semi-governmental and private sector corporations (Maddineni & Ragi, 2011). These believe is supported by statistics that leads to the same conclusion.

The results of the assessment have shown major discrepancies in the cyber security paradigm of the two organizations. If sustained, these cyber security discrepancies will lead to breaches in confidentiality, integrity or availability of information resources (Maddineni & Ragi, 2011).

1. Mitigating such discrepancies is possible by applying security techniques listed in the conclusion of Chapter four for the specific case of the two organizations assessed. Other organizations may require more or less mitigations depends on the shape of their cyber security paradigm.
2. The mitigations required costs organization "Alpha" and organization "Beta" a huge number of resources in terms of manpower, capital expenditure cost of projects and continue operations cost. Taking into consideration that cyber security is a

very rapid evolving topic and the security model that is suitable for today is not definite to be suitable for tomorrow, costs will keep increasing. Organizational management requests their IT personnel to consider alternative solutions (Dawoud, et al., 2010).

3. The alternative solution that is discussed and proposed in this thesis is the utilization of cloud computing. Although cloud has been widely used recently, but the idea of subcontracting supporting services that are not the core business of an organization is a very old strategy for businesses and organizations resources (Maddineni & Ragi, 2011).
4. In the two case studies of organization "Alpha" and organization "Beta", it was obvious that they were welling to subcontract IT projects and operations requirement. Going into cloud is a further step into which the whole IT service is sub contracted.
5. Before going into details of the cloud solution, cyber security should be evaluated. Advantages and Disadvantages in addition to the ability to solve the current cyber security issues and keep a well maintained up to date security model should be presented for the case studied in this thesis.
6. In Chapter three, it is stated that all cyber security techniques in cloud computing is applied and most of the data centers that provides cloud computing services will have solutions that covers all of the security issues found in the assessment. The mitigation for these issues, or inherited issues as identified in chapter three, is because of certain reasons that are also listed in the same chapter such as staff dedication and availability of resources.

Studying effect on existing cyber security issues when migrating to cloud is half of the picture only (Maddineni & Ragi, 2011). In order to have the whole picture clear, introduced cyber security

issues that is related to the nature of the cloud services should be assessed for organization "Alpha" and "Beta" to migrate to cloud safely and with convince.

Cyber security introduced issues are discussed such as exposure to public networks and loss of control. These issues have mitigations as well. It all depends on the cloud service provider for which the methodology for selecting the provider is important (Maddineni & Ragi, 2011). For organization "Alpha" and organization "Beta" assessed in this thesis, the recommendation is to form a governmental cloud company that uses the community service model for governmental institutes and provides IaaS for storage services as a deployment model. Details are in the following section. The Last section of this chapter has specific solutions for cyber security introduced issues because of cloud.

7. Based on this study, organization "Alpha" and "Beta" should be convinced of the cyber security benefits they will have from migrating to cloud service following the service model and deployment model suggested in this thesis. There are certain things to be considered in migration to cloud. The following section also considers high level plan and contractual issues related to such a project.

5.5.2 Cloud Migration Proposal

Organizations must concentrate on the following steps in considering cloud services:

1. Analyze organizational requirement for IT services and cloud services specifically. Apply international codes, standards, and guidelines. National Institute of Standards and Technology (NIST) (Mell & Grance, 2011), European Telecommunication Standards

Institute ETSI, and International Telecommunication Union (ITU) are examples of prestigious international standardization organizations that have published standards for different aspects of cloud computing.

2. Assess, select, engage and later oversee the cloud service that best suit the requirement. Normally cloud services are considered to achieve certain goals that mainly revolve around two points: cost reduction and efficiency growth. Security is supposed to be an area where compromises will take place in favor of cost and efficiency. At the same time, due to the rapid and heavy increase in cyber security risks, cyber security systems have evolved (Leavitt, 2009).

In order to achieve security in systems that are maintained locally, an organizational line should be established and a lot of efforts, cost and procedures should be taken place which may deviates the organization from its goals. Except for the fact that the data is in other organizational premises and communication means are required (Both leads to a number of security issues that have been discussed), it is found in this thesis that security enhanced positively by migrating storage services to cloud, because of the lack of ability to control the cyber security risks, technologies and the requirements for the in-house systems (Kumar, et al., 2012).

On the other hand, and as stated earlier cloud introduces new cyber security threats that should be addressed and tackled in the right way in order to get all of the benefits of cloud without compromising security and this is addressed in the following major recommendations of this proposal.

Addressing Cloud Computing Risks

The consumer should form a task force for risk management to deal with cyber security risks associated to the utilization of cloud services.

This task force will have inputs to the service contract components required (Kumar, et al., 2012).

Servicing data-center location

One of the most important recommendations related to the service is the knowledge of the location of the data and applications. Some cloud providers have datacenters in different countries and the services provided for a consumer including the storage service may be provided by resources of more than one data center located in two different countries (Antonopoulos & Gillam, 2010). Although the different locational data centers belongs to the same cloud provider but each data center in every country are subjected to the laws and regulations of that country. A consumer whose data is important cannot withstand such a risk nor follow up the laws and regulations of other countries (Antonopoulos & Gillam, 2010). The situation becomes worst when the data centers hosting a consumer's data is in a country that is not known for the consumer. This issue should be stated clearly in the service contract and followed up by audits and reviews.

Monitoring by Provider

The consumers in general are very proactive in stating confidentiality agreement within the cloud service contracts that preserves the data of the company from being revealed to third parties. In contrast, consumers are less concerned about restricting monitoring activities of service provider itself.

Cloud services provider should be prevented by law and contract terms and condition from wide monitoring capabilities to the data. In general, some monitoring tools are required even by the consumer specifically virus and malicious software monitoring and related stuff (Antonopoulos & Gillam, 2010).

Quality of Service Assurance

A high level of cyber security paradigm level cannot be ensured unless certain level of quality assurance in place and guaranteed.

Quality assurance should have certain criteria of quality for each and every category of the service including but not limited to availability, performance and recovery.

Service Agreement

Service agreements or contracts are the most important framework that defines the cloud service right stand duties of the consumer and the provider. Service agreements define the specifications and arrangements of the service (Zhou, et al., 2010).

For companies and institutes that manages their services in-house and do not rely on cloud services providers, internal policies and procedures covers almost the same aspects that are covered and set by the service agreement when cloud services are in use.

The following are some of the topics that must be defined in service agreements (Zhou, et al., 2010):

- Terms and Conditions of use and access
- Period of Service
- Renewal and Termination conditions

In some occasions, service agreements are distributed among several agreement documents such as service level agreement, terms of use, and acceptable and privacy policy. The reason for which service agreements are mentioned here as a building block for the proposed secure cloud solution for storage services is that security is highly dependent on the terms defined in the service agreement.

There are two important recommendations related to service agreements that should be followed by companies and institutes in order to have a robust secure cloud service:

1. Non-Negotiated Agreements should not be used.

In predefined service agreements, terms are prescribed by service providers only and are not negotiable. A definite result would be an agreement that is more towards the provider interest and typically lack terms that protects consumer security and privacy (Kennedy & Gopal, 2010). Moreover, in some cases provider have the right to change the terms without the need to consult users and consumers. Such service agreements are very much popular on public cloud services.

Negotiable service agreement is a must for companies and institutes that have security as an important priority. Negotiating the terms in the service agreements paves the way to have full control over security by ensuring that all inherited and introduced cyber security issues that have been discussed in chapter five are addressed. The following are some points that can improve cyber security and should be negotiated in the service agreement preparation stage (Revoredo, et al., 2013):

- Policy of Security and Privacy
- Procedure of Security and Privacy
- Technical Controls
- Ownership of Data
- Breach notification, and much more

2. Professional technical and legal consultation should be utilized. The terms of the service agreement highly affects the specifications of the cloud service including the cyber security aspect. In order to have a service agreement that ensures that all current and future cyber security requirements are met, it is important to have a specialized legal and technical teams within the negotiation team force (Antonopoulos & Gillam, 2010).

Deployment Strategy

Specifically for the case of organizational storage requirement, particularly governmental organizations, under consideration and that have been assessed in this thesis, private cloud deployment or community is suggested to be utilized.

In the assessment, one of the organizations was not interested in migrating to cloud services due to its cautiousness about confidentiality. The other organization's network specialist was a little bit easier in that aspect but he may phase difficulties in the management approvals stage due to the same concern. The proposal that is suggested in this thesis for governmental organizations or other organizations that are under one umbrella, is to have a community cloud that is managed by government for governmental institutions or managed by a company that belongs to the same corporate for private organizations.

Most of the developed countries including many countries in the region as well have adopted the solution of having a national data center to provide cloud services for critical governmental institution and in that aspect it is a community cloud deployment method .which have been introduced in chapter three of this thesis.

5.5.3 Mitigations against introduced cyber security threats of cloud computing

- Shared Multi-Tenant Environment (Revoredo, et al., 2013) :
    - High level of assurance of the security mechanisms protecting the logical separation
    - Utilizing community or private deployment model of cloud computing
- Public Networks exposed Services (Revoredo, et al., 2013):

- Limiting the exposure surface to the minimum possible limit: the priority would be for organizational-owned communication channel. If this option is not possible, then a dedicated channel that belongs to a telecommunication utility is recommended.
- Having an assured minimum bandwidth limit on the communication channel to guarantee the availability required.
- Having a different security and communication scheme for administrative access.

- Loss of Control (Revoredo, et al., 2013):
  - For strong legally-backed contract that assures a full compliance by cloud service provider to consumer organization policies and procedures and laws and regulations.
  - Continues audit and monitoring of the activities of the cloud service provider.
  - Effective reporting mechanism from service provider to consumer that is enforced by the service contract.

In addition, a very essential task to do is the common practices of continuous audits and reviews that are should be supported and agreed in the terms of the service agreement.

Chapter 6: Conclusion and Future Work

6.1 Thesis Conclusion

6.2 Future work

Chapter 6: Conclusion and Future Work

This chapter presents the contributions of the thesis and suggests areas into which further research is required.

6.1 Conclusion

In this thesis, a risk assessment model for cyber security of local storage systems has been proposed. The model is based on the idea of cyber security domains and criterions. The proposed model has been implemented in two organizations by interviewing organizations' specialists and acquiring answers to the assessment questionnaire. The risk assessment implementations results have showed risks of different ratings in the cyber security of local storage systems of the assessed organizations.

Risks have been identified. Security techniques required to mitigate the identified risks have been discussed. It is found that those techniques and the nature of rapid evolution in cyber security attacks and threads impose high demand of resources overhead on the organizations. In the thesis, utilization of cloud for storage services is addressed. The cyber security aspect of such utilization is thoroughly studied. This study has considered the effect on current security issues in local storage systems and introduces issues due to the nature of cloud computing services.

It is found that the utilization of cloud computing for storage systems results in a model that is free of all cyber security breaches and vulnerabilities found in the assessment of the organizations' local storage systems. It is found also that such utilization introduces new cyber security issues related to the nature of cloud computing. Other aspects of migrating storage services to cloud have been briefly introduced including cost and performance. However, the research done in this thesis has concentrated only on the information security aspect.

The thesis is concluded with a proposal for secure utilization of cloud computing for organizational storage requirements. The proposal takes into consideration many aspects of cloud services contracts and technological requirements. Deployment model, service model, service contract and mitigations for introduces cyber security issues are all part of the proposal presented. In conclusion, it is found that proper utilization of cloud computing for storage services for organizations is the most appropriate approach for organizations nowadays.

6.2 Future work

Based on the research done in this thesis, a lot of research tracks can be introduced and contributes to the worldwide researchers' efforts in this field. One research track would be proposing a scientific risk assessment methodology similar to the one proposed in this thesis but for cloud computing based storage services. The assessment would be of two parts one of which has a questionnaire to be answered by service provider and the other to be answered by service consumer to have the holistic picture clear.

Another approach would be interrelated more factors other than cyber security in storage systems local and cloud implementations study. As a conclusion of the research done and literature review it is believed that extra work is required in the field of standards and regulations in cloud computing specialized services including storage services. This field requires tremendous research efforts as well.

References

Alexander Pickering, A., & Cowley, S. (2010). Risk Matrices: implied accuracy and false assumptions, *Journal of Health & Safety Research & Practice*, 2(1), 9-16.

Ateeq, A. (2012). Type of Security Threats and It's Prevention, *International Journal of Computer Technology & Applications*, 3(2), 750-753.

Ahmadi, M.R., & Maleki, D. (2010). Effect of Virtual Techniques in Data Storage Access, *IEEE 24th International Conference on Advanced Information Networking and Applications Workshops (WAINA)*, Perth, 91-96.

Antonopoulos, N., & Gillam, L. (2010). *Cloud computing: principles, systems and applications*, London, Springer Science & Business Media.

Behl, A. (2011). Emerging security challenges in cloud computing: An insight to cloud security challenges and their mitigation, *2011 World Congress on Information and Communication Technologies (WICT),* Iumbai, 217-222.

Bhardwaj, A., & Kumar, V. (2011). Cloud Security Assessment and Identity Management, *14th International Conference on Computer and Information Technology (ICCIT)*, Dhaka, 387-392.

Bensoussan, K., & SingRu, H.(2011). Impact of security risks on cloud computing adoption, Communication, *49th Annual Allerton Conference on Control and Computing (Allerton)*, Monticello, 670-674.

Bhisikar, P. & Sahu, A. (2013). Security in Data Storage and Transmission in Cloud Computing, *International Journal of*

Advanced Research in Computer Science and Software Engineering, 3(3), 410-415.

Bilski, T. (2007). A Formal Model for Data Storage Security Evaluation, *ICCS International Conference* on *Computational Science and its Applications,* Kuala Lampur, 253-257.

Dinadayalan, P., Jegadeeswari, S. , & Gnanambigai, D. (2014). Data Security Issues in Cloud Environment and Solutions, *2014 World Congress on Computing and Communication Technologies (WCCCT)*, Trichirappalli, 88-91.

Dawoud, W., Takouna, I., & Meinel, C. (2010). Infrastructure as a service security: Challenges and solutions, *The 7th International Conference on Informatics and Systems (INFOS),* Cairo,1-8.

Elva, M. (2012, April 27). A New Risk Measurement, retrieved from http://abscompliance.blogspot.com.

Eight to Late. (2009). Cox's Risk Matrix Theorem and its Implications for Project Risk Management, retrieved from https://eight2late.wordpress.com/2009/07/01/cox%E2%80%99s-risk-matrix-theorem-and-its-implications-for-project-risk-management/.

Gnanasundaram, S., & Shrivastava, A. (2012). *Information Storage and Management*, Canada, John Wiley & Sons, Inc.

Goda, K., & Kitsuregawa, M. (2012). The History of Storage Systems, *Proceedings of the IEEE,* 100, 433-1440.

ISO/IEC 27000:2009 (E). (2009). Information technology - Security techniques - Information security management systems - Overview and vocabulary. ISO/IEC.

Jansen, W., & Grance, T. (2011). Guidelines on Security and Privacy in Public Cloud Computing, *National Institute of Standards and Technology Gaithersburg*, 1-80.

John R.M, & Tolga, A. (2000). Security Domains: Key Management in Large-Scale Systems, *IEEE Software,* 17 (5), 52-58.

Koletka, R., & Hutchison, A. (2011). An Architecture for Secure Searchable Cloud Storage, *Information Security South Africa (ISSA),* Johannesburg, 1-7.

Kumar, A. & Byung, G. L., HoonJae, L., & Kumari, A. (2012). Secure storage and access of data in cloud computing, *International Conference on ICT Convergence (ICTC)*, Jeju Island, 336-339.

Leavitt, N. (2009). Is Cloud Computing Really Ready for Prime Time, *IEEE Computer*, 42 (1),15-20.

Liu, W. (2012). Research on cloud computing security problem and strategy, *2nd International Conference on Consumer Electronics, Communications and Networks (CECNet)*, Yichang,1216-1219.

Maddineni, V., & Ragi, S. (2011). *Security Techniques for Protecting Data in Cloud Computing,* Blekinge Institute of Technology.

Moyo, M., Abdullah, H., & Nienaber, R.C. (2013). Information security risk management in small-scale organisations: A case study of secondary schools computerised information systems, *Information Security for South Africa*, Johannesburg, 1-6.

Miller, E., Long, D., Freeman, W., & Reed, B. (2001). Strong security for distributed file systems, *IEEE International Conference on Performance, Computing, and Communications*, Phoenix, AZ, 34-40.

Mathur, P., & Nishchal, N. (2010). Cloud computing: New challenge to the entire computer industry, *1st International Conference on Parallel Distributed and Grid Computing (PDGC)*, Solan, 223-228.

Muppala, J.K. ,Hiltunen, M., Robert, S. Wang, J.(2011). The First International Workshop on Dependability of Clouds, data centers and Virtual Computing Environments, *IEEE/IFIP 41st International*

Conference on Dependable Systems & Networks (DSN), Hong Kong, 590-591.

Mell, P., & Grance, T. (2011*). The NIST Definition of Cloud Computing*, National Institute of Standards and Technology, 1-7.

Online digital solution (ODSI). (2013). Retrieved from *http://www.odsi.co.uk/blog/wp-content/uploads/2013/08/History-of-computer-data-storage.png.jpg, 2014.*

Kennedy, R., & Gopal, T.V. (2010). Assessing the risks and opportunities of Cloud Computing Defining identity management systems and maturity models, *IEEE Trends in Information Sciences & Computing (TISC*), Chennai,138-142.

Public Safety Canada, Emergency Management Planning Guide 2010–2011, http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-mngmnt-pnnng/mrgnc-mngmnt-pnnng-eng.pdf

Revoredo da Silva, C.M. Costa da Silva, J.L., Rodrigues, R.B. ,Medeiros Campos, G.M. , Marques do Nascimento, L., & Cardoso Garcia, V.(2013). Security Threats in Cloud Computing Models: Domains and Proposals, *IEEE 6th International Conference on Cloud Computing (CLOUD),* Santa Clara, 383-389.

Elva, M. (2012, April 27). A New Risk Measurement, retrieved from http://abscompliance.blogspot.com.

Riedel, E., Kallahalla, M., & Swaminathan, R. (2002). A framework for evaluating storage system security, *1st Conference on File and Storage Technologies (FAST), Monterey, CA.*

Stanton, P. (2004). Securing Data in Storage: A Review of Current Research, *ACM Computing Research Repository (CoRR)*, 1-22.

Sadiku, M.N.O., Musa, S.M., & Momoh, O.D. (2014). Cloud computing: opportunities and challenges, *IEEE Potentials,* 33 (1), 34-36.

Stambul, M.A.M. (2011). An assessment model of information security implementation levels, *International Conference* on *Electrical Engineering and Informatics (ICEEI)*, Bandung, 1-6.

Microsoft (2000). Security Threats, retrieved from http://msdn.microsoft.com/en-us/library/cc723507.aspx, 2014.

Sitaram, D., & Manjunath, G. (2011). *Moving To the Cloud: Developing Apps in the New World of Cloud Computing*, retrieved from http://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/mrgnc-mngmnt-pnnng/index-eng.aspx, 2014.

Usman, M., & Ayub, R. (2012). *Cloud Computing as a Tool to Secure and Manage Information Flow in Swedish Armed Forces Networks*, Blekinge Institute of Technology, 1-465.

Wang, C., Wang, Q., Ren, K., & Lou, W.(2009). Ensuring Data Storage Security in Cloud Computing, *17th International Workshop on Quality of Service, IWQoS*, Charleston, 1-9.

Zhou, M., Zhang, R., Wei Xie, Qian, W., & Zhou, A. (2010). Security and Privacy in Cloud Computing: A Survey, *Sixth International Conference on Semantics Knowledge and Grid (SKG)*, Beijing, 105-112.

Gupta, P., & Kaur, A.(2013). An Enhanced Security Technique for Storage of Multimedia Content over Cloud Server, *International Journal of Engineering Research and Applications (IJERA)*, 3 (4), 2273-2277.

Appendix A. Local Storage Systems Assessment Questionnaire

1. Pre-Assessment Questionnaire for Storage Systems Custodians

1. How many Storage Systems you have?
2. What types of Storage Systems you have?
3. What are the purposes of the Storage Systems?
4. What is the frequency of access to every storage system?
5. What is the data flow rate of every Storage System?
6. What is the capacity of every Storage System?
7. What Hardware you are using for each type?
8. What OS/Softwares each Storage System have?
9. Do you have service contracts with external companies for managing/licensing/supporting?
10. Do you have dedicated staff for storage systems?
11. How many people/man-hours you are dedicating for storage systems?
12. Have you considered the option of using Cloud storage services? Why?

2. Questionnaire for Information Security Systems Custodians

Application Access Security Domain

Criterion 1: Controlling User Access to data

Threats: User/Host Spoofing identity of another User/Host, Elevating privilege of existing User/Host

Impact: Minor

Questionnaire to Storage System Cyber security Custodians:

1. Do you have Technical controls for User/Host Authentication for data access?
2. Do you have Technical controls for User/Host Authorization?
3. Is your User/Host Authentication/Authorization controls centralized or it resides on the storage system itself? On other words, do you have strong Enterprise Identity management system that manages Authentication and Authorization processes?
4. Is your User/Host Authorization process controlled by Administrative procedures?
5. Do you have an Account management/Password management procedure for Users/Hosts?
6. Do you have Access Control Lists on the Storage System?
7. Do you have virtual LANs on the network that restricts Users/Hosts access?
8. Do you have regular auditing over the technical and administrative controls for Users/Hosts?
9. Do you have security logging for all Users/Hosts access activities?
10. Do you prevent Users/Hosts from accessing these security logs?

11. Do you have a centralized continuously monitored center in which these logs aggregate?

Criterion 2: Protecting the Storage Infrastructure

Threats: Unauthorized Host/User Getting access, Spoofing identity of existing User/Host, Snooping Network, Executing Attacks

Impact: Minor

Questionnaire to Storage System Cyber security Custodians:

1. Is your physical infrastructure secured in access controlled buildings?
2. If your storage system is accessible wirelessly. Are you using a secure wireless protocol?
3. Are your networks devices secure from unauthorized connections?
4. Do your network devices report any unauthorized node connection attempts?
5. Do you have a continuously monitored centralized security center that aggregates such attempts in early stages?
6. Is data on your storage network encrypted? IPSec or FC-SP secures protocols for example.
7. Do you have Role-Based Access Control RBAC? Do you have personnel who can add users to storage systems other than those whose role is to manage users?
8. Do you have a separation of duties procedure/policy? Can the person who authorizes the addition of accounts be the same person that uses them or configure them?
9. Is your management network separated logically from enterprise network? For example, segregation using firewalls, routers and virtual LANs.

Criterion 3: Data Encryption

Threats: Thieving Data Media, Tampering with data

Impact: Moderate

Questionnaire to Storage System Cyber security Custodians:

1. Do you encrypt data on the storage system?
2. Does the encryption happen prior to being transferred to Storage disk?
3. Do you have write off procedure for data on disks that have reached end of life? Are you confident when disposing Storage disks that data cannot be reconstructed?
4. Do you have Antivirus engines on your storage system?
5. Do you have other software controls on the Storage system that ensures data integrity? For example, the use of MD5 or SHA-256 cryptography algorithm.
6. Is the Storage System physically secured in an access control environment?

Management Access Security Domain

Criterion 1: Controlling Administrative Access

Threats: User/Host Spoofing identity of another User/Host, Elevating privilege of existing User/Host

Impact: Major

Questionnaire to Storage System Cyber security Custodians:

1. Do you have access control applied on all Storage system components?
2. Do you have a strong third-party authentication system such as Active Directory?

3. Do you have power users with different privileges to pursue different roles?
4. Is an administrator access required for routine tasks?
5. Do you have Role Based Access Control RBAC applied?
6. Do you have a centralized monitoring system that aggregates all security logs?
7. Does administrative action logs have higher priority logs and grabs attention of security monitoring personnel?
8. Do your event logs have high security levels as your data?
9. Do you have a centralized time server that synchronizes all Storage infrastructure devices to allow tracking of logs and events?

Criterion 2: Protecting the Management Infrastructure

Threats: Unauthorized Host/User Getting access, Spoofing identity of existing User/Host, Snooping Network, Executing Attacks

Impact: Major

Questionnaire to Storage System Cyber security Custodians:

1. Is your management traffic encrypted?
2. Do you have a separate network segment for management traffic?
3. Do you have access control on network management segments?
4. Do you use Firewalls, Routers and Virtual LANs to protect access to management segments?
5. Is the number of hosts that have access to management segments minimized and restricted?
6. Do you have access control on the storage system to specify which host has management access to which Storage array?

7. Do you have in-packet inspection devices interfacing storage system to allow certain commands from certain hosts and prevent others?
8. Do you have regular activity to disable unused network services on the Storage infrastructure?

Backup, Replication and Archive Security Domain

Threats: Thieving Data Media, Spoofing Disaster Recovery Site Identit.

Impact: Moderate

Questionnaire to Storage System Cyber security Custodians:

1. Do you have remote site (Disaster Recovery Site) that has a live connection to the storage system? If not, do you have a remote location to which you send frequently backups of your Storage system?
2. Does your remote location sustain same Technological and Physical security standards as your Storage System location?
3. If you have a remote replication site, is the communication protocol secure? Is the communication channel dedicated?
4. Does your backup solution encrypt the data?
5. If you have tape backups, do you have strict procedure for handling of the tapes?
6. Does the backup Media have authentication mechanisms to be restored?
7. Do you have restoration and validation tests procedure to ensure backups integrity?

3. Supporting Questionnaire for discussion and conclusions

1. Does the Storage System Administration Team is also responsible of the cyber security of Storage Systems?
2. Do you have dedicated personnel for cyber security? Is cyber security part of the IT organizational Chart? Or does it report to another entity in the organization?
3. Does the governing part of cyber security (Policies/Procedures/Audits) responsibility is with the cyber security implementation responsibility handled by one entity?
4. As a percentage, how do you rate the cyber security goals of your storage system (Confidentiality, Integrity, Availability and Accountability)?
5. Are the resources available to support the demand on storage systems sufficient? Have you ever faced an issue with the availability of data because of the demand?
6. Do you have resources for continuous monitoring of alerts and logs for storage systems?
7. When security system or a security measure is proposed to be deployed, does the cost of it be challenged along with the value of

information being secured? Is it also validated from external security consultant?

8. Do you have scheduled plans for penetrations test or Cyber security reviews by third parties? On what frequency?
9. Do you have appointed personnel for communication with the CERT Computer Emergency Response Team or the responsible Authority in your country? Are you considered to be critical infrastructure that is audited from cyber security point of view from government?
10. Have you had cyber security incident ever? What have the incident (If applicable) compromised (Confidentiality, Integrity or Availability)? Can you share with me the incident investigation outcomes?
11. Do you benchmark your cyber security framework against competitive organizations?
12. Do you have a schedule for cyber security preventive maintenance (Updates, Patches, Definitions, and fixes)? Have you automated some of these measures?
13. Have you had an incident because a schedule was not followed because of lack in manpower?
14. Do you have disaster recovery plans in place for all of your systems? Do you emergency locations for operation? Is the staff

trained on such a plan? Is it part of a holistic business continuity management plan for the organization?

15. Have you gone through risk surface reduction process for any of your storage systems? Have it resulted in minimizing exposure to internet or WAN networks?

16. Have you conducted Cyber security awareness sessions for your IT personnel?

17. Do you have obsolesance management plan? Do you have resources (Hardware/Software) that is already obsolete?

18. Do you have coordination with the physical security department to review the access list of personnel for these rooms?

19. Do you have data retention policy that is followed for all of the data stored on storage systems?

20. When a system is decommissioned? How do you deal with hard disks or storage media? Do you have a policy/procedure for the erasure mechanism?

Appendix B. Alpha Case Study, Information Security of Local Storage Systems

Organization name is hidden in this thesis because of the sensitivity of information that is related to the cyber security of their systems. Name of the interviewed personnel is hidden also due to the same reason.

This assessment has been conducted on 12th of March 2014 along with the network specialist in the organization.

The person interviewed was the network specialist of the organization. The network specialist has had his bachelor degree in Business Information systems in 2009. He has more than five years of experience in the field of IT systems. He has a wide range of certificates in the fields of project management, Microsoft systems, Auditing, networks and network security.

1. Pre-Assessment Questionnaire for Storage Systems Custodians

Questions Related to Storage Systems in General:

1. How many Storage Systems you have?

   We have four storage systems in place.

2. What types of Storage Systems you have?

   We have the following storage systems:

   a. 1 NAS

   b. 2 SAN

   c. Tape

3. What are the purposes of the Storage Systems?
    a. NAS: The NAS is used for backup and restore purposes.
    b. 2 SAN: The SAN is used for servers and applications data storage.
    c. Tape: Tapes are used for storing backups.
4. What is the frequency of access to every storage system?
    a. NAS: Daily Use
    b. 2 SAN: Daily Use
    c. Tape: Daily Use
5. What is the data flow rate of every Storage System?

    The data flow rate is approximately 50 to 100 GByte weekly.
6. What is the capacity of every Storage System?

    The storage systems have a total of

    a. NAS: 25 TB
    b. 2 SAN: 15TB/10TB
7. What Hardware you are using for each type?

    For SAN we use a DELL and an IBM storage system and for NAS we are using a DELL system and we use HP system as a tape drive.
8. What OS/Softwares each Storage System have?

    Our storage systems are windows based systems.

9. Do you have service contracts with external companies for managing/licensing/supporting?

   Yes. We have a variety of contracts that manages different aspects of our IT infrastructure some of which affects the storage system. We utilize agreements services for Hosting, Network maintenance and applications maintenance. We have also licensing agreements with companies for Microsoft, Cisco ad McAfee.

10. Do you have dedicated staff for storage systems?

    No

11. How many people/man-hours you are dedicating for storage systems?

    We have two personnel that have multiple responsibilities in terms of systems including handling storage systems.

12. Have you considered the option of using Cloud storage services? Why?

    Yes. We have a development plan with a cloud service provider to have a cloud platform that hosts some of our application, documents, workflows, website, and collaboration tools.

2. Questionnaire for Information Security Systems Custodians

Application Access Security Domain

Criterion 1: Controlling User Access to data

Questionnaire to Storage System Information Security Custodians:

1. **Do you have Technical controls for User/Host Authentication for data access?**

   Yes
2. **Do you have Technical controls for User/Host Authorization?**

   Yes
3. **Is your User/Host Authentication/Authorization controls centralized or it resides on the storage system itself? On other words, do you have strong Enterprise Identity management system that manages Authentication and Authorization processes?**

   Yes
4. **Is your User/Host Authorization process controlled by Administrative procedures?**

   Yes
5. **Do you have an Account management/Password management procedure for Users/Hosts?**

   Yes
6. **Do you have Access Control Lists on the Storage System?**

   Yes
7. **Do you have virtual LANs on the network that restricts Users/Hosts access?**

   No
8. **Do you have regular auditing over the technical and administrative controls for Users/Hosts?**

   Yes

9. **Do you have security logging for all Users/Hosts access activities?**

   Yes

10. **Do you prevent Users/Hosts from accessing these security logs?**

    Yes

11. **Do you have a centralized continuously monitored center in which these logs aggregate?**

    No

Criterion 2: Protecting the Storage Infrastructure

Questionnaire to Storage System Information Security Custodians:

1. **Is your physical infrastructure secured in access controlled buildings?**

   Yes

2. **If your storage system is accessible wirelessly. Are you using a secure wireless protocol?**

   No we don't have wireless (NA)

3. **Are your network devices secure from unauthorized connections?**

   Yes

4. **Do your network devices report any unauthorized node connection attempts?**

   Yes

5. **Do you have a continuously monitored centralized security center that aggregates such attempts in early stages?**

   No

6. **Is data on your storage network encrypted? IPSec or FC-SP secure protocols for example.**

   No

7. **Do you have Role-Based Access Control RBAC? Do you have personnel who can add users to storage systems other than those whose role is to manage users?**

   No

8. **Do you have a separation of duties procedure/policy? Can the person who authorizes the addition of accounts be the same person that uses them or configure them?**

   Yes

9. **Is your management network separated logically from enterprise network? For example, segregation using firewalls, routers and virtual LANs.**

   No

Criterion 3: Data Encryption

Questionnaire to Storage System Information Security Custodians:

1. **Do you encrypt data on the storage system?**

   No

2. **Does the encryption happen prior to being transferred to Storage disk?**

   No

3. **Do you have write off procedure for data on disks that have reached end of life? Are you confident when disposing Storage disks that data cannot be reconstructed?**

   No

4. **Do you have Antivirus engines on your storage system?**

   No for SAN, Storage servers Yes.

5. **Do you have other software controls on the Storage system that ensures data integrity? For example, the use of MD5 or SHA-256 cryptography algorithm.**

No

6. **Is the Storage System physically secured in an access control environment?**

   Yes

Management Access Security Domain

Criterion 1: Controlling Administrative Access

Questionnaire to Storage System Information Security Custodians:

1. **Do you have access control applied on all Storage system components?**

   Yes

2. **Do you have a strong third-party authentication system such as Active Directory?**

   Yes

3. **Do you have power users with different privileges to pursue different roles?**

   No

4. **Do you prohibit the use of administrator account for routine jobs such as adding and deleting users?**

   No

5. **Do you have Role Based Access Control RBAC applied?**

   Yes

6. **Do you have a centralized monitoring system that aggregates all security logs?**

   No

7. **Does administrative action logs have higher priority logs and grabs attention of security monitoring personnel?**

   No

8. **Do your event logs have high security levels as your data?**

Yes

9. **Do you have a centralized time server that synchronizes all Storage infrastructure devices to allow tracking of logs and events?**

   No

Criterion 2: Protecting the Management Infrastructure

Questionnaire to Storage System Information Security Custodians:

1. **Is your management traffic encrypted?**

   No

2. **Do you have a separate network segment for management traffic?**

   No

3. **Do you have access control on network management segments?**

   Yes

4. **Do you use Firewalls, Routers and Virtual LANs to protect access to management segments?**

   Yes

5. **Is the number of hosts that have access to management segments minimized and restricted?**

   Yes

6. **Do you have access control on the storage system to specify which host has management access to which Storage array?**

   Yes

7. **Do you have in-packet inspection devices interfacing storage system to allow certain commands from certain hosts and prevent others?**

   Yes

8. **Do you have regular activity to disable unused network services on the Storage infrastructure?**

   No

Backup, Replication and Archive Security Domain

Questionnaire to Storage System Information Security Custodians:

1. **Do you have remote site (Disaster Recovery Site) that has a live connection to the storage system? If not, do you have a remote location to which you send frequently backups of your Storage system?**

   No

2. **Does your remote location sustain same Technological and Physical security standards as your Storage System location?**

   No

3. **If you have a remote replication site, is the communication protocol secure? Is the communication channel dedicated?**

   No

4. **Does your backup solution encrypt the data?**

   No

5. **If you have tape backups, do you have strict procedure for handling of the tapes?**

   No

6. **Does the backup Media have authentication mechanisms to be restored?**

   No

7. **Do you have restoration and validation tests procedure to ensure backups integrity?**

   No

3. Supporting Questionnaire for discussion and conclusions

1. Does the Storage System Administration Team is also responsible of the information Security of Storage Systems?

   Yes

2. Do you have dedicated personnel for information security? Is information security part of the IT Organizational Chart? Or does it report to another entity in the organization?

   No separate section for information security. It is part of the duties of IT department personnel.

3. Does the governing part of information security (Policies/Procedures/Audits) responsibility is with the information security implementation responsibility handled by one entity?

   Yes. All are handled by IT only.

4. Are the storage infrastructure resources available to support the demand on storage systems sufficient? Have you ever faced an issue with the availability of data because of the demand?

   Yes the resources are sufficient and we had not face issues with availability.

5. Do you have resources for continuous monitoring of alerts and logs for storage systems?

   No

6. When security system or a security measure is proposed to be deployed, does the cost of it be challenged along with the value of information being secured? Is it also validated from external security consultant?

   Yes but not always and not for all systems.

7. Do you have scheduled plans for penetrations test or Information security reviews by third parties? On what frequency?

   Yes we do internal and external penetration tests yearly.

8. Do you have appointed personnel for communication with the CIO or the responsible Authority in your country? Are you considered to be critical infrastructure that is audited from information security point of view from government?

   We have personnel for communication, No its not critical infrastructure.

9. Have you had information security incident ever? What have the incident (If applicable) compromised (Confidentiality, Integrity or Availability)? Can you share with me the incident investigation outcomes?

   Yes we had couple of incidents. We had viruses that have been detected, clients that had not get the antivirus update in time.

10. Do you benchmark your information security framework against competitive organizations?

No

11. Do you have a schedule for information security preventive maintenance PM (Updates, Patches, Definitions, and fixes)? Have you automated some of these measures?

Yes we do PM activities and most of them are automated.

12. Have you had an incident because a schedule was not followed because of lack in manpower?

No

13. Do you have disaster recovery plans in place for all of your systems? Do you emergency locations for operation? Is the staff trained on such a plan? Is it part of a holistic business continuity management plan for the organization?

No

14. Have you gone through risk surface reduction process for any of your storage systems? Have it resulted in minimizing exposure to internet or WAN networks?

No

15. Have you conducted Information security awareness sessions for your IT personnel?

Yes

16. Do you have obsolesance management plan? Do you have resources (Hardware/Software) that is already obsolete?

No.

17. Do you have data retention policy that is followed for all of the data stored on storage systems?

No.

18. When a system is decommissioned? How do you deal with hard disks or storage media? Do you have a policy/procedure for the erasure mechanism?

We try to recover data from hard disks and storage media at last we have support. No we don't have.

4. Assessment Results Table

	Criterion	Impact	# of Questions	Not Applicable	Positive	Negative	Probability Calculation	Probability	Risk
Application Access Security Domain	*Controlling User Access to data*	Minor	11	0	9	2	0.181818182	Unlikely	Low
	Protecting the Storage Infrastructure	Minor	9	1	4	4	0.5	Moderate	Low
	Data Encryption	Moderate	6	0	1	5	0.833333333	Likely	Moderate
Management Access Security Domain	*Controlling Administrative Access*	Major	9	0	4	5	0.555555556	Moderate	Moderate
	Protecting the Management Infrastructure	Major	8	0	5	3	0.375	Moderate	Moderate
Backup, Replication and Archive Security Domain	*Backup, Replication and Archive Security Domain*	Moderate	7	0	0	7	1	Likely	Moderate

Appendix C. Beta Case Study, Information Security of Local Storage Systems

Organization name is hidden in this thesis because of the sensitivity of information that is related to the cyber security of their systems. Name of the interviewed personnel is hidden also due to the same reason.

This assessment has been conducted on 12th of March 2014 along with an IT representative in the organization.

This IT representative holds the position of senior infrastructure and network administrator in the organization. He has got his bachelor degree in engineering informatics in 2009 followed by a master degree in computer science in 2012. He has gone through five years of experience in the field of IT systems. He has wide range of certificates in IT systems such as Cisco Certified Network Associate (CCNA) in networks, Microsoft Certified Solutions Associate (MCSA) in Microsoft solutions and Symantec backup Exec (SBE) in Symantec backup and recovery solutions

1. Pre-Assessment Questionnaire for Storage Systems Custodians

Questions Related to Storage Systems in General:

1. How many Storage Systems you have?

   We have three storage systems.

2. What types of Storage Systems you have?

   We have the following storage systems:

   a. NAS

b. SAN

c. Tape

3. What are the purposes of the Storage Systems?

   a. NAS: The NAS storage is used as a file server to archive different types of files.

   b. SAN: The SAN is used for servers and applications data storage.

   c. Tape: Tapes are used for storing backups.

4. What is the frequency of access to every storage system?

   a. NAS: Daily Use

   b. SAN: Daily Use

   c. Tape: Incremental (Daily), Deferential (Weekly) and Full back up (Yearly)

5. What is the data flow rate of every Storage System?

   a. NAS: 1 GByte Daily

   b. SAN: 10 GByte Daily

   c. Tape: 8 GByte as per the frequency of access specified in the previous question

6. What is the capacity of every Storage System?

   a. NAS: 8 TBytes

   b. SAN: 8 TBytes

7. What Hardware you are using for each type?

For the NAS and SAN we use Fujitsu and the tape drive is HP

8. What OS/Softwares each Storage System have?

   The operating system of the NAS and SAN is Linux Kernel and the tape drive is embedded system.

9. Do you have service contracts with external companies for managing/licensing/supporting?

   Yes. We have different types of agreements such as an Enterprise agreement with Central Informatics Organization (CIO), maintenance agreement for Network devices, and another Maintenance agreement for upgrades and troubleshooting. In addition, we have agreement for web hosting for our website and other agreements for Software licensing.

10. Do you have dedicated staff for storage systems?

    No

11. How many people/man-hours you are dedicating for storage systems?

    No dedication. Man-hours depend on requirements.

12. Have you considered the option of using Cloud storage services? Why?

    No. Because we are highly concerned of the confidentiality of our data and the connection speed that current infrastructure allows.

2. Questionnaire for Information Security Systems Custodians

Criterion 1: Controlling User Access to data

Questionnaire to Storage System Information Security Custodians:

1. **Do you have Technical controls for User/Host Authentication for data access?**

   Yes

2. **Do you have Technical controls for User/Host Authorization?**

   Yes

3. **Is your User/Host Authentication/Authorization controls centralized or it resides on the storage system itself? On other words, do you have strong Enterprise Identity management system that manages Authentication and Authorization processes?**

   Yes. We have a centralized domain controller

4. **Is your User/Host Authorization process controlled by Administrative procedures?**

   Yes

5. **Do you have an Account management/Password management procedure for Users/Hosts?**

   Yes

6. **Do you have Access Control Lists on the Storage System?**

   Yes

7. **Do you have virtual LANs on the network that restricts Users/Hosts access?**

   Yes

8. **Do you have regular auditing over the technical and administrative controls for Users/Hosts?**

No

9. **Do you have security logging for all Users/Hosts access activities?**

   Yes

10. **Do you prevent Users/Hosts from accessing these security logs?**

    Yes

11. **Do you have a centralized continuously monitored center in which these logs aggregate?**

    No

Criterion 2: Protecting the Storage Infrastructure

Questionnaire to Storage System Information Security Custodians:

1. **Is your physical infrastructure secured in access controlled buildings?**

   Yes

2. **If your storage system is accessible wirelessly. Are you using a secure wireless protocol?**

   NA

3. **Are your network devices secure from unauthorized connections?**

   Yes

4. **Do your network devices report any unauthorized node connection attempts?**

   Yes specially the firewall and gateway devices

5. **Do you have a continuously monitored centralized security center that aggregates such attempts in early stages?**

   Yes.It is called SCOM from Microsoft

6. **Is data on your storage network encrypted? IPSec or FC-SP secure protocols for example.**

   No

7. **Do you have Role-Based Access Control RBAC? Do you have personnel who can add users to storage systems other than those whose role is to manage users?**

   No

8. **Do you have a separation of duties procedure/policy? Can the person who authorizes the addition of accounts be the same person that uses them or configure them?**

   Yes we have.

9. **Is your management network separated logically from enterprise network? For example, segregation using firewalls, routers and virtual LANs.**

   No

Criterion 3: Data Encryption

Questionnaire to Storage System Information Security Custodians:

1. **Do you encrypt data on the storage system?**

   No

2. **Does the encryption happen prior to being transferred to Storage disk?**

   No

3. **Do you have write off procedure for data on disks that have reached end of life? Are you confident when disposing Storage disks that data cannot be reconstructed?**

   Yes

4. **Do you have Antivirus engines on your storage system?**

No , everybody can access the data stored in Storage devices through the authorized server there is antivirus on the mention server

5. **Do you have other software controls on the Storage system that ensures data integrity? For example, the use of MD5 or SHA-256 cryptography algorithm.**

   No

6. **Is the Storage System physically secured in an access control environment?**

   Yes

Management Access Security Domain

Criterion 1: Controlling Administrative Access

Questionnaire to Storage System Information Security Custodians:

1. **Do you have access control applied on all Storage system components?**

   Yes

2. **Do you have a strong third-party authentication system such as Active Directory?**

   Yes

3. **Do you have power users with different privileges to pursue different roles?**

   No

4. **Do you prohibit the use of administrator account for routine jobs such as adding and deleting users?**

   No

5. **Do you have Role Based Access Control RBAC applied?**

   No

6. **Do you have a centralized monitoring system that aggregates all security logs?**

   No

7. **Does administrative action logs have higher priority logs and grabs attention of security monitoring personnel?**

   No

8. **Do your event logs have high security levels as your data?**

   Yes

9. **Do you have a centralized time server that synchronizes all Storage infrastructure devices to allow tracking of logs and events?**

   Yes its called active directory

Criterion 2: Protecting the Management Infrastructure

Questionnaire to Storage System Information Security Custodians:

1. **Is your management traffic encrypted?**

   No

2. **Do you have a separate network segment for management traffic?**

   No

3. **Do you have access control on network management segments?**

   Yes

4. **Do you use Firewalls, Routers and Virtual LANs to protect access to management segments? Yes we use all the mention in the question**

5. **Is the number of hosts that have access to management segments minimized and restricted? Yes of course**

6. **Do you have access control on the storage system to specify which host has management access to which Storage array?**

Yes

7. **Do you have in-packet inspection devices interfacing storage system to allow certain commands from certain hosts and prevent others?**

   We are using IPS\IDS enable firewall and host enable too

8. **Do you have regular activity to disable unused network services on the Storage infrastructure? No**

Backup, Replication and Archive Security Domain

Questionnaire to Storage System Information Security Custodians:

1. **Do you have remote site (Disaster Recovery Site) that has a live connection to the storage system? If not, do you have a remote location to which you send frequently backups of your Storage system?**

   Yes

2. **Does your remote location sustain same Technological and Physical security standards as your Storage System location?**

   Yes

3. **If you have a remote replication site, is the communication protocol secure? Is the communication channel dedicated?**

   Yes

4. **Does your backup solution encrypt the data?**

   No

5. **If you have tape backups, do you have strict procedure for handling of the tapes?**

   No

6. **Does the backup Media have authentication mechanisms to be restored?**

No. The resources are not sufficient for the demand in terms of bandwidth and other factors as well. We have come into situation where the data was not available due to the demand.

5. Do you have resources for continuous monitoring of alerts and logs for storage systems?

   No

6. When security system or a security measure is proposed to be deployed, does the cost of it be challenged along with the value of information being secured? Is it also validated from external security consultant?

   Yes. The cost is challenged internally without validation from external consultant.

7. Do you have scheduled plans for penetrations test or Information security reviews by third parties? On what frequency?

   No. Not for storage systems.

8. Do you have appointed personnel for communication with the CIO or the responsible Authority in your country? Are you considered to be critical infrastructure that is audited from information security point of view from government?

   Yes. We have effective communication with CIO and we are considered to be critical organization.

9. Have you had information security incident ever? What have the incident (If applicable) compromised (Confidentiality, Integrity or Availability)? Can you share with me the incident investigation outcomes?

   We had a security incident but sorry I can't share any information about it (thanks for understanding)

10. Do you benchmark your information security framework against competitive organizations?

    We do not have benchmark against competitive organization but we do benchmark our framework against international standards including ISO standard.

11. Do you have a schedule for information security preventive maintenance PM (Updates, Patches, Definitions, and fixes)? Have you automated some of these measures?

    Yes we do PM activities and most of them are automated.

12. Have you had an incident because a schedule was not followed because of lack in manpower?

    No

13. Do you have disaster recovery plans in place for all of your systems? Do you emergency locations for operation? Is the staff trained on such a plan? Is it part of a holistic business continuity management plan for the organization?

Yes

14. Have you gone through risk surface reduction process for any of your storage systems? Have it resulted in minimizing exposure to internet or WAN networks?

Yes

15. Have you conducted Information security awareness sessions for your IT personnel?

Yes

16. Do you have obsolesance management plan? Do you have resources (Hardware/Software) that is already obsolete?

No. We do not have a plan but when we came across obsolesance situation for switches and firewalls for instance we have replaced them.

17. Do you have data retention policy that is followed for all of the data stored on storage systems?

Yes

18. When a system is decommissioned? How do you deal with hard disks or storage media? Do you have a policy/procedure for the erasure mechanism?

We have a procedure that manages this issue.

4. Assessment Results Table

	Criterion	Impact	# of Questions	Not Applicable	Positive	Negative	Probability Calculation	Probability	Risk
Application Access Security Domain	*Controlling User Access to data*	Minor	11	0	9	2	0.181818182	Unlikely	Low
	Protecting the Storage Infrastructure	Minor	9	1	5	3	0.375	Moderate	Low
	Data Encryption	Moderate	6	0	2	4	0.666666667	Likely	Moderate
Management Access Security Domain	*Controlling Administrative Access*	Major	9	0	4	5	0.555555556	Moderate	Moderate
	Protecting the Management Infrastructure	Major	8	0	5	3	0.375	Moderate	Moderate
Backup, Replication and Archive Security Domain	*Backup, Replication and Archive Security Domain*	Moderate	7	0	4	3	0.428571429	Moderate	Moderate

ملخص الرسالة

تعتمد المؤسسات في الوقت الحاضر على الأنظمة المعلوماتية بما فيها أنظمة تخزين البيانات. من النادر جدا وجود منظمة لا تمتلك نظاما لتخزين البيانات. نظام تخزين البيانات لا يعتبر فقط نظاما لأرشفة الملفات وإنما يعتبر ركن أساسي تعتمد عليه معظم أنظمة المعلومات الحديثة كأنظمة البريد الإلكتروني, وأنظمة قواعد البيانات بالإضافة إلى أنظمة التطبيقات المتنوعة. في الوقت ذاته يعتبر أمن وحماية المعلومات من القطاعات التي تتطور بسرعة كبيرة جدا بالاضافة الى أهميتها الناتجة عن تأثيرها على جميع أنظمة المعلومات التي تمتلكها المؤسسات.

بالإضافة إلى ما ذكر سابقا تعتبر الحوسبة السحابية أحد أهم التطورات التي حدثت في تقنية المعلومات في السنوات الأخيرة . تنتمي الحوسبة السحابية الى عائلة خدمات التعاقد من الباطن. تحبذ المؤسسات التعاقد مع شركات خارجية للإستفادة من خدماتها في القطاعات الخارجة عن العمل الرئيسي لهذة المؤسسات..تقدم هذه الاطروحة نظاما لتقييم مستوى أمن وحماية المعلومات في أنظمة التخزين الحالية التي تعتمدها المؤسسات. هذا التقييم هو نتاج لعمليات بحث دؤوبة في مجالات أمن المعلومات وتقنيات تخزين البيانات. تستعرض كذلك الأطروحة نتائج تطبيق نظام التقييم على إثنتان من المنظمات الهامة في مملكة البحرين.أثبتت النتائج التي تم استنتاجها أن أنظمة تخزين البيانات تحتوي على ثغرات امنية قد تعرضها لمخاطر من مستويات مختلفة. نسبة كبيرة من الأسئلة التي تضمنها استبيان أجيبت بشكل سلبي من قبل الإدارات المسؤولة في المؤسسات التي خضعت للتقييم. نستنتج من هذه النتائج أن المؤسسات غير قادرة على مواكبة التطور السريع في أمن وحماية المعلومات وحماية أنظمة تخزين البيانات الخاصة بهم. طرحت الأطروحة كذلك إستخدام خدمات الحوسبة السحابية لاستضافة أنظمة التخزين وناقشت الأطروحة فوائد انتقال خدمات التخزين من الأنظمة الحالية الى السحابة الإلكترونية. بالإضافة إلى ذلك تم مناقشة التأثير على أمن المعلومات الناتج عن هذا الانتقال. توصلت الأطروحة إلى نتيجة مهمة وهي أن الانتقال بخدمات التخزين الى السحابة الإلكترونية يحل معظم الثغرات الأمنية في أنظمة التخزين الحالية التي تمتلكها المؤسسات. إن جهود البحث العلمي التي بذلت في هذه الأطروحة أدت إلى اقتراح توصيات شاملة للمؤسسات للمضي قدما بمتطلبات التخزين الخاصة بهم آخذين بالاعتبار أمن المعلومات بالإضافة إلى مستويات التكلفة والكفاءة والأداء.

جامعة البحرين
المكتبة
LIBRARY
University of Bahrain

جامعة البحرين

كلية تقنية المعلومات

تحسين امن اجهزة خزن البيانات باستخدام الحوسبة السحابية

مخطط بحث لاستكمال متطلبات الحصول على درجة الماجستير

في تقنية المعلومات

إعـــــداد

حنين محمد عبدالله

الرقم الجامعي:20114653

إشـــــراف

وسن شاكر عواد

(أستاذ مشارك)

جامعة البحرين

مملكة البحرين

ديسمبر 2014