B.Sc. in Computer Science and Engineering Thesis

Assesment of Information Technology Security Management System: A Case Study of Military Institute of Science and Technology

Submitted by

MD. Nazib Mahmud Shajib
ID: 201114004

Sadi Mohammad Zaman
ID: 201114022

Nabid Salman
ID: 200914025

Supervised by

Jahidul Arafat

Lecturer

Department of Computer Science and Engineering

Military Institute of Science & Technology, Dhaka-1216

Bangladesh

Department of Computer Science and Engineering
Military Institute of Science and Technology

December 2014

CERTIFICATION

This thesis paper titled **"Assesment of Information Technology Security Management System: A Case Study of Military Institute of Science and Technology"**, submitted by the group as mentioned below has been accepted as satisfactory in partial fulfillment of the requirements for the degree B.Sc. in Computer Science and Engineering in December 2014.

Group Members:

MD. Nazib Mahmud Shajib

Sadi Mohammad Zaman

Nabid Salman

Supervisor:

Jahidul Arafat
Lecturer
Department of Computer Science and Engineering
Military Institute of Science & Technology, Dhaka-1216
Bangladesh

•

CANDIDATES' DECLARATION

This is to certify that the work presented in this thesis paper, titled, "Assesment of Information Technology Security Management System: A Case Study of Military Institute of Science and Technology", is the outcome of the investigation and research carried out by the following students under the supervision of Jahidul Arafat, Lecturer, Department of Computer Science and Engineering, Military Institute of Science & Technology, Dhaka-1216, Bangladesh.

It is also declared that neither this thesis paper nor any part thereof has been submitted anywhere else for the award of any degree, diploma or other qualifications.

MD. Nazib Mahmud Shajib
ID: 201114004

Sadi Mohammad Zaman
ID: 201114022

Nabid Salman
ID: 200914025

ACKNOWLEDGEMENT

We are thankful to Almighty Allah for his blessings for the successful completion of our thesis. Our heartiest gratitude, profound indebtedness and deep respect go to our supervisor, Jahidul Arafat, Lecturer, Department of Computer Science and Engineering, Military Institute of Science & Technology, Dhaka-1216, Bangladesh, for his constant supervision, affectionate guidance and great encouragement and motivation. His keen interest on the topic and valuable advices throughout the study was of great help in completing thesis.

We convey our special thanks to the reviewers for their constructive review and guidelines.

We are especially grateful to the Department of Computer Science and Engineering (CSE) of Military Institute of Science and Technology (MIST) for providing their all out support during the thesis work.

Finally, we would like to thank our families and our course mates for their appreciable assistance, patience and suggestions during the course of our thesis.

Dhaka
December 2014

MD. Nazib Mahmud Shajib

Sadi Mohammad Zaman

Nabid Salman

ABSTRACT

Information security (IT) is an intense issue of modern day, due to drastic increasing application of computer, internet and internet user and intrusions. Various IT security approaches have been invented on this aspect while among them Soft IT Security approach (SITS) along with Robust IT Security-Balancing(RITS-B) approach are highly lucrative now-a-days due to its simplicity and effectiveness in the sector of Information security especially in Higher Education. Besides, Information technology security in higher education has become more of a management issue of securing the higher education environment without affecting the data integrity, accessibility, academic and intellectual freedom which is the core of the higher education environment. Most recent trend suggest that Higher Education has a larger number of reported breaches among all sectors thus resulting an increased potential threats in upcoming days. Being an emerging state of IT in Higher Education in Bangladesh the empirical research scope on this field is a no denying fact. This paper has focused on case study of IT security environment from the mentioned perspective to draw on the direct experience of those able to provide insights into strategies, policies and practices of MIST and the efforts those they have emphasized more to secure their information arena. The case study systematically addressed many of the challenges brought more sharply into focus by information technologies from organizational value, belief and practice aspects. It has opened up few unsettled issues in present state of IT security environment of Higher Education framework of MIST to persuade them for future research for attaining a globally satisfactory shape for higher education information security.

TABLE OF CONTENT

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1
INTRODUCTION

Information Technology (IT) security Management System in higher education is the process of securing the higher education management system without affecting the data integrity, accessibility, academic and intellectual freedom which is the core of the higher education management system . It is about preserving confidentiality, assuring information integrity and lastly making data accessible to authorized users on a timely basis. Despite the numerous functionality of security, IT security in Higher education is still a subject of ongoing investment. It cannot be conclusively stated that education field is highly secured because of the stakeholders interest, application, technological and intrusions diversity. Most recent trend suggest that Higher Education Has a Larger Number of Reported Breaches among all sectors thus resulting an increased potential threats in upcoming days. Assessing an IT security management system of a Higher education institute (e.g. Engineering Institute) can help the organization identifying its current IT security management system resulting an improved IT Security management and execution framework.

1.1 Background of the Research

Information Technology (IT) security is an emerging field of research in recent days. IT security breaches raising, thus raising the concerns of business and educational environments [1]. Several security approaches has been defined and many approaches has made to cover the major security concerns on protecting the data and information. But none could fit the all concerns. On this,Clarke and Furnell [2] has covered the major Information Technology Security Approaches available in the literature. Most of the security schemes can be roughly categorized into two approaches:

- The Hard i.e. Technical Method
- The Soft i.e. Non-Technical Method

The first approach fails to gain total effectiveness in the higher education information security process due to mainly budgetary constraints and people-technology integration problems [3]. The strategies for the second approach exploit the importance of soft IT interven-

tions (e.g. organization, Cultural aspects, awareness program, training programs, policies, executive attention etc.) to produce a secured campus management system around the educational institution. Second approach has advantages such as: (a) It is very simple in nature (b) It evaluates all the spatial properties of Information security. (c) Representation of security pattern is much more effective and well-structured than only technology based security processing. (d) It gives dynamic and formalized solution to security concerns. (e) It is based on the belief that openness and accessibility of higher education management system will not only be preserved but also be secured. The features of this approach provide well organized security solution with some limitations on Concerns and generalization because of academic and departmental diversities.

To improve the security scheme, a strategy consists in combining these approaches in order to obtain a robust security by exploiting the advantages of one method to overcome the limitations of the other one. This is an attempt to asses an IT security management system basing on unified methods of higher education information security approaches under a common topology based on the both hard and soft interventions.

The Unauthorized Disclosure of information to individuals not authorized to view such data continues to be the leading type of information security incident that colleges and universities suffer at large. The top three most common types of incidents within higher education accounted for 95% of all of the incidents in 2009 [4].A Case study revealed that few of the challenges that MIT faces are: (a) Wireless technology (b) Vendors dont necessarily incorporate security in a usable way (c) Difficulty in quantifying the value of security (d) Restricted information access fosters illegally stored data on desktops. (e) Response time decrease (d) Prepare for future [5]. Thus comes the necessity of IT security assessment and defensive measures thereon. Thereby this study has been undertaken to in-depth the IT security benchmarks in Military Institute of Science and Technology (MIST) and to provide insights into policies, technologies, and practices those they have adopted and those believed could strengthen their IT security supports.

1.2 Statement of the Problem

This study deals with the information technology security behaviors, practices and policies of MIST. MIST being an institution of Bangladesh armed forces has inputs lots of promises on the potential growth of education and research. But it often faces the dilemmas of what exactly to do with the IT security and where they should have emphasized more. Thereby this study in the form of a case analysis in-depth on how the organization can be facilitated with an improved IT Security management and execution framework. It has assessed the IT security polices, practices and strategies of MIST and the efforts those they have emphasized

more to secure their information arena.

1.3 Significance of the Research

IT strategic plan devises the execution steps for an Institutes IT security. When we know Firewall cant alone give security to all devices connected in a secure network of a University, rather creates false state of security in IT planners mind. What we really need is integrity of computing resource from unauthorized access. With increasing wireless access threat to intrusion has increased rapidly, especially in a management system like frequent data uses in a University. Therefore, need to assess the strength and weaknesses according to security culture and organization functioning in an Institute has become a basic study requirement for Security Researcher.

Present study might lead to an exemplary IT security practices that can only be attained with a clear understanding of who needs or wants access to what and of the types of security measures that should be in place to protect sensitive data and the system on which the data live. This was intended to identify the vulnerabilities while promoting security awareness among information users of MIST and among similar other educational institutions.

1.4 Scope of the Research

This research includes assessment of MIST security polices, awareness program, current environment, IT security enterprise process, incident handling procedure, risk assessment, external services or consulting on IT security, IT security funding, outcomes of IT security management, issues/future directions of IT security management and enhancement across MIST. This effort believes to enable the IT security practitioner of MIST to reassess their technological investment while reshaping the security awareness and user behavior across the campus. Following three disturbances will be considered for the generation of data set: (a) Disturbance 1: intrusions in the exiting information transaction system of MIST, causing the system to act vulnerable (b) Disturbance 2: Threats in the exiting information transaction system of MIST, causing the system to be penetrated and compromised; (c) Disturbance 3: User behaviors those cause the raise of penetration, intrusion and act as threat.

A case study on MIST gives an in-depth knowledge on the current security priority on temporal and spatial basis. Therefore, it can assist in decision making process to integrate work in higher education with national effort to strengthen critical infrastructure and empowering members of the institutions community to do their work securely.

1.5 Research Context

Universities often run systems with vulnerabilities and little monitoring or management. The typical university research or teaching lab is managed by a faculty member who has many other responsibilities or by a student manager who may have had little training. Universities are havens for free exchange of ideas. Thus, their access controls typically are configured to promote sharing and wide access to a population that changes significantly every semester. A worse problem is that universities are really loose federations of departments and research groups. The administrator for one group's computers may not even know other administrators, let alone share intelligence or tools. Often, computers are bought for a teaching or research project, but there is not funding for ongoing maintenance, either buying upgrades or installing patches. The large and frequently changing university student body gives the attacker great opportunity to maintain anonymity while developing an attack [6].

When most of the educational institutions carry out research; confidentiality and ensuring secure distribution and integrity of their data is an utmost need in todays' excelling technological management system. MIST with the vision to enhance the educational excellence of Bangladesh is named to be a pioneer organization run under Ministry of Defence. With its unique characteristics it features lots of confidentiality while as an institutions it also promises the information to be visible to all. Thereby the need to assess the IT security management system across the campus came up with great priority. The study focuses on to enhance the overall IT strategy, policy and practice to asses and shape up to counter security threat and vulnerabilities.

1.5.1 Purpose of the Research

The purpose of this research is to briefly assess the IT security investments and practices within the academic and administrative arena of MIST. It focused on how to improve the security scheme, what strategies could be adopted and how all those has been combining to ensure a robust security around the information arena of MIST. Thereby this study believes to input significant contribution on the information security efforts of MIST. It also has emphasized on how to enhance the security benchmarks of MIST and how the institution could protect their information assets with an enriched security framework.

1.5.2 Research Aim

The aim of this research was to give us a better understanding of Information Technology Security, Strategies and Practices in MIST and to suggest an improved and more secured IT management system.

1.5.3 Research Objectives

General Objective

The general objective of this study is to assess the present strength and weaknesses of case institutions IT security management system. It focused on how to improve the security scheme, what strategies could be adopted and how all those has been combining to ensure a robust security around the case arena.

Specific Objective

- To identify the information technology security governance, strategies and practices of MIST.
- To evaluate the strength and challenges of present IT security management practices.
- To facilitate the organization with an improved IT Security management and execution framework.
- To motivate users and aware them with an easy-to-use mobile application on secured IT behavior.

1.5.4 Research Questions

- What are the scope of information technology security within the information arena of MIST?
- What types of security tools academia is currently using?
- How effective are the strategy, policy and practices of MIST to protect its information assets?
- How to merge the institutions cultural layout with that of its existing hard framework to satisfy security requirement with ethical concerns?

1.6 Delimitation of the Study

This study solely focused on the IT security polices, practices and strategies those being adopted in MIST to secure their information assets and to aware their users on security vulnerabilities. It delimits its scope on how to improve the security scheme, what strategies could be adopted and how all those could have been combined to ensure a robust security around the case arena.

1.7 Definition of the used terms

Information Security- By far the most commonly used meaning for information security is the preservation of (a) Confidentiality or protection from unauthorized use or disclosure of information (b) Integrity, ensuring data accuracy and completeness through protection from unauthorized, unanticipated, or unintentional modification, and including authenticity and (c) Availability, making data available to the authorized users on a timely basis and when needed [5, 7, 8].

Hard Intervention- One of the Information Security Scheme that is ensured by technical method with common tools that includes antivirus software, SSL for web transactions, centralized data backup, network firewall, enterprise directory, VPN for remote access, intrusion detection and prevention tools, encryption, content monitoring filtering, electronic signature and shibboleth [9].

Soft Intervention- One of the Information Security Scheme that is ensured by non-technical methods like organization, Cultural aspects, awareness program, training programs, policies, executive attention, policies etc. to produce a secured management system around the institution [9].

1.8 Structure of the Dissertation

This paper is organized on five chapters. Chapters including an introduction, literature review, research methodology, result, analysis and discussion and conclusion with a recommendation. A summary of these individual chapters is details below.

Chapter 1, Introduction- the outline were presented to bring the reader in common line with the core of the research topic. It also identified the pin-point of our research scope along with objectives.

Chapter 2, Literature review- this is related to the basic idea on higher education IT security including their advantages and disadvantages assessed from critical point of view. This chapter identified what is already known about the area of study, questioned a body of research does not answer and made strong case for why further study of research questions is important on this field.

Chapter 3, Research Methodology- Selection criteria and reasoning were presented here that best suited our purpose in a logical manner.

Chapter 4, Results, Analysis and Discussion- The main part was to analyze the data derived

and the results to be furnished along with appropriate and brief case discussion, which were solely done in chapter 4.

Chapter 5, Conclusion and Recommendation- This chapter has concluded the findings, results and discussions made so far in the previous chapters and sections. It has recommended several techniques and strategies for overcoming the information security drawbacks of MIST in its subsequent sections and subsections. It also has mentioned the future scope of study in this related arena of research.

CHAPTER 2
LITERATURE REVIEW

Literature review can be explained as the systematic explanation of knowledge that is available on the given topic. It helps in gaining information and insight to the chosen topic and not gets influenced by one's own perspective, agenda or personal interest. This chapter is of extreme importance for the literature review to be complete and not to take any sides. Also, this chapter paves light on various techniques and dynamics of researches that are conducted on the topics of similar nature.

2.1 Structure of the Literature Review

This chapter highlighted on factors for users to use the information security facility at MIST within the boundary of IT security strategy, policy and practice. They were assessed with their IT security awareness and behavior. In Bangladesh all kind of free internet facility are favorite to students, which makes them clearly vulnerable to any kind of information and data theft including mail id or social media account hacking, theft of personal and commercial data, images etc. The internet users are increasing day by day in Bangladesh, so does the incidents of information security breaching. The faculty and other users also needed to act securely over IT environment. A sense of IT security among all user of MIST IT environment must therefore be integrated.

2.2 Theoretical Framework of References

Though there are huge numbers of Information security balancing approaches in the literature the Soft IT Security (SITS) approaches on the acceptable use of security scheme [9]. Hard interventions are only considered in subsequent for discussion purpose with present technological measures that form modern IT security core of approaches. This study basically featured theoretical framework that asses the IT security management system of MIST keeping focus on implemented strategy, policy and practices to adopt soft intervention. For this reason, the related literature based on the IT security approaches was presented in the subsequent paragraphs.

2.2.1 What is information Security?

By far the most commonly used meaning for information security is the preservation of :(a) Confidentiality or protection from unauthorized use or disclosure of information.(b) Integrity, ensuring data accuracy and completeness through protection from unauthorized, unanticipated, or unintentional modification, and including authenticity. (c) Availability, making data available to the authorized users on a timely basis and when needed. Preservation of confidentiality, integrity and availability of information [5, 7, 8]. In addition, other properties, such as authenticity, accountability, non-repudiation and reliability can also be involved [10].

Threats to information and information systems may be categorized and a corresponding security goal may be defined for each category of threats. A set of security goals, identified as a result of a threat analysis, should be revised periodically to ensure its adequacy and conformance with the evolving management system. The currently relevant set of security goals may include: confidentiality, integrity, availability, privacy, authenticity & trustworthiness, non-repudiation, accountability and auditability [11].

2.2.2 What for the Information Security Management System?

The governing principle behind an Information Security Management System (ISMS) is that an organization should design, implement and maintain a coherent set of policies, processes and systems to manage risks to its information assets, thus ensuring acceptable levels of information security risk. As per security experts [12]:

- Information technology security administrators should expect to devote approximately one-third of their time addressing technical aspects. The remaining two-thirds should be spent developing policies and procedures, performing security reviews and analyzing risk, addressing contingency planning and promoting security awareness;
- Security depends on people more than on technology;
- Employees are a far greater threat to information security than outsiders;
- Security is like a chain. It is only as strong as its weakest link;
- The degree of security depends on three factors: the risk you are willing to take, the functionality of the system and the costs you are prepared to pay;
- Security is not a status or a snapshot, but a running process.

These facts inevitably lead to the conclusion that security administration is a management issue, and not a purely technical issue.

Information security management will enable implementing the desirable qualitative characteristics of the services offered by the organization (i.e. availability of services, preservation of data confidentiality and integrity etc.). By preventing and minimizing the impacts of security incidents, ISMS ensures business continuity, customer confidence, protect business investments and opportunities or reduce damage to the business.

2.2.3 Different Patterns of Information Security Management System

Most Prominent IT security approaches that are commonly used for both Wired and Wireless IT security are-Network Firewall(Perimeter),Network Firewall(Interior),Enterprise directory, Electronic Signature, Shibboleth, Encryption, Centralized data backup system, Virtual Private Network(VPN) for remote access, Security Standards for application or system development, Secure Socket Layer(SSL) for secure web transactions, Intrusion Detection, Intrusion prevention tools, Active content monitoring, Secure Remote Password protocol (SRP), Wired Equivalency Privacy(WEP),Extensive Authentication Protocol(EAP), Internet Protocol VPN(IP VPN),Kerberos. Notable that these are mainly Hard or Technology centric approaches. Among those mentioned above few of the most popular system/approach are discussed here.

(a) **Firewalls-** A firewall is a device that blocks Internet communications access to a private resource. The private resource can be a network, a server or a personal computer. A firewall allows unfettered outbound packets from, say, a protected network to the Internet world, but allows only appropriate inbound packets. Firewalls are popular and effective, but can be subverted if the protected resource has modem configured for auto-answer. There are two types of firewalls protocol-level firewalls and application-level firewalls [13].

(b) **Virtual Private Networks (VPN)-** VPNs provide a secure, dynamic tunnel capability that allows users to make use of both the Internet and a protected LAN simultaneously without the worry of exposing sensitive information to cybercriminals. Using IPSecs tunnel mode, VPNs encrypt the source and destination addresses of a packet so that these are not exposed to Internet hackers as clear text but are still usable for routing purposes. Typically, todays solutions apply the Data Encryption Standard (DES) algorithm or extended 3DES scheme to maximize the length of keys used to scramble and unscramble data, although newer standards are emerging, e.g. Advanced Encryption Standard (AES). AES specifies key lengths of 128-bits, 192-bitsand 256-bits8 [13].

(c) **Intrusion Detection Systems-** Another way to fortify perimeter defense is to install an IDS, especially on core systems like e-mail, web and domain name servers. Intrusion detection systems supplement firewall technology with strong monitoring and record keeping at both the network and host levels. IDS technologies monitor network traffic and system logs to compare whats going on in real-time to the known methods of hackers. When a suspicious event is detected, an alarm is kicked off immediately. However, hackers have shown firm resolve to break new defenses when the bar is raised [13].

(d) **Shibboleth-** Shibboleth is a 'single-sign in', or logging-in system for computer networks and the Internet. It allows people to sign in, using just one 'identity', to various systems run by 'federations' of different organizations or institutions. The federations are often universities or public service organizations. The Shibboleth Internet2 middleware initiative created an architecture and open-source implementation for identity management and federated identity-based authentication and authorization (or access control) infrastructure based on Security Assertion Markup Language (SAML). Federated identity allows the sharing of information about users from one security domain to the other organizations in a federation. This allows for cross-domain single sign-on and removes the need for content providers to maintain user names and passwords. Identity providers (IdPs) supply user information, while service providers (SPs) consume this information and give access to secure content.

(e) **Kerberos-** Kerberos is a computer network authentication protocol which works on the basis of 'tickets' to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Its designers aimed it primarily at a clientserver model and it provides mutual authenticationboth the user and the server verify each other's identity. Kerberos protocol messages are protected against eavesdropping and replay attacks. MIT continues to implement its security strategy using Kerberos, X.509 certificates, and strong machine- and application-based defenses.

The above all facts argued for creativity and continual improvement of a multi-level defense system to meet the goal of protecting an organizations information assets.

2.2.4 What is Higher Education IT Security Management System?

Higher education, post-secondary education, tertiary education or third level education is an optional final stage of formal learning that occurs after secondary education. It is taken to include undergraduate and postgraduate education. Often delivered at universities, academies, colleges, seminaries, and institutes of technology, higher education is also available through

certain college-level institutions, including vocational schools, trade schools, and other career colleges that award academic degrees or professional certifications. The Higher education management system mostly means Knowledge management system: incorporating social practices, technological and physical arrangements intended to facilitate collaborative knowledge building, decision making, inference or discovery. It may also include Social management system: the culture that an individual lives in, and the people and institutions with whom they interact. Basically, the management system to be focused can be summarized as technical management system and non-technical management system for the present day higher education arena. It includes the external and internal users, system and all associated stakeholders.

2.2.5 Current Image of the Higher Education Information Security Management System

Focusing strictly on technology trends can obscure other environmental factors that are drivers for innovation in higher education. The following ten major issues in the landscape of present Higher Education Information Management System that are creating areas of potentially drastic changes and also seeking attention for security are [14]: (a) The Increasing Differentiation of Higher Education. (b) The Transformation of the General Education Curriculum. (c) The Faculty Faces of the Future. (d) The Surge in Global Faculty and Student Mobility. (e)The New ”Invisible College”. (f) The Changing ”Traditional” Student. (g) The Mounting Pressure to Demonstrate the Value Added of a College Degree. (h) The Revaluation of ”Middle-Skill” Jobs. (i) Higher Education as a Private Rather Than a Public Good. (j)Lifelong Partnerships with Students.

Current recommendation on IT Security management system is that organizations must concentrate on developing metrics for the top-four security issues identified from the survey results [15]: (a) Phishing (b) Compliance issues (c) BYOD (Bring Your Own Device) or mobile device management (d) Data loss/leakage prevention. It has become more difficult to bring everyone under security protocol/policies because of more rapidity and dynamism in technologies that are integrating both the teachers and the students almost every day.

2.2.6 Development Initiatives of Higher Education Information Security System

We are living in the era where affordable, easy-to-use, and readily accessible technologies facilitate a bring-your-own everything (BYOE) standard in the workplace and in the learning management system. Bringing your own technology has been and continues to be the norm for students, and it is becoming the norm for faculty and staff [15].

The proliferation of user-provisioned technologies does not change the basic best prac-

Table 2.1: Case Study on Higher Education Security Breech.

Case Study	Problem Statement	Awareness Effort	Measured Results
Emory University	Emory University saw that compromised accounts due to phishing attacks were a constant source of problems and that their approach of using posters and traditional awareness messages was not effective.	Emory used a fee-based phishing service to target their customers with phishing messages as a security awareness effort.	Over three rounds of phishing campaigns, Emory community members showed a 40.9% decrease (improvement) in the number of customers who supplied their credentials to the phishing messages.
University of North Carolina	The University of North Carolina at Wilmington was ranked third among all 17 universities within the UNC system in DMCA violations	To address this issue, supplemental education was incorporated into a layered awareness campaign for incoming students.	The data gathered showed a decrease of 71% in violations during the first month of implementing the new security awareness education program, and a 95% decrease in violations in the second month.
Texas State University	As an action item from a data loss incident, Texas State University began a Securing Confidential Data awareness and training campaign while concurrently implementing technology to reduce future exposures.	A training workshop was developed and presented to departments on campus that were known to handle confidential information	Three months after implementing e-mail DLP, the number of outgoing confidential messages was reduced by 50%; six months after implementing this solution, there was an 80% reduction in outgoing confidential e-mail.

Source:ECAR Study of Undergraduate Students and Information Technology,2013

tices around security very much a solid security presence and plan on campus can adjust to most BYOE challenges. The fears of BYOE being the cause of a virus spreading throughout a campus network or of sensitive data being stolen, corrupted, or lost are often misplacedthe real cause is likely a straight-up security vulnerability that transcends BYO technologies [15].Accordingly, Risk Management is suggested into four steps-(a) Securing Data (b) Managing Access(c) Securing Systems and Networks (d) Managing Identity and Authentication. On the other hand User Awareness has three steps-(a) Raising User Awareness (b) Educating Users (c) Enforcing Compliance. Subsequent paragraphs elaborated the development initiatives in an orderly fashion.Few of the related case study problems, efforts and results are shown in Table 2.1

Risk Management- For securing data, they should reside on secure servers, be encrypted at rest and in transit and only be accessed through secure applications or https. To manage the access it is needed to be an active stakeholder to enterprise-level systems, services and data. Role-based access and multifaceted institutional oversight authorizing personnel to access secure data and mission-critical systems should be well defined, understood, and followed. For securing systems and network firstly the Local data centers should be secured via key/keycard, access given based on roles and security of data centers is formally monitored. Secondly, Security audits should be routine, frequent, systematic, and comprehensive. To Identity management effort Institutional priorities for identity management standards should be in sync with the capacity to effectively manage identities.

User Awareness- For raising user awareness one should be an advocate for educating oneself about BYOE security concerns. Then he/she should motivate the adoption of smart security practices by addressing personal security issues simultaneously with institutional security issues. Educating user is done by engaging them in activities that raise user awareness of security issues. Institute should have well-written, easily understood, and widely accessed policies on security for BYOE but good policy may not always translate into good security. Enforcement of compliance can be monitored, and policies are enforceable. If policy compliance can neither be tracked nor enforced, then repackaging the policy information as guidelines or suggested use/behavior may be prudent.

2.2.7 Current Scale, Scope and Diversity of the Information Security Management System in Higher Educational Information Management System of Bangladesh

In the recent past an alleged website hacking incident of MIST was observed by amateurish effort but needed to act promptly and with due care [16]. Few of the alleged hacked sites-Bangladesh Public Service Commission (BPSC), Information and Communication Technology Division, Pabna Textile Engineering College, University Grant Commission (UGC) and few other- became victimized to the cyber-attack from Hackers [17]. Normally website hacking threat are still in a limited scale and at random level, even though the matter need to get serious concern at such primary level. Shahjalal University of Science and Technology (SUST), Dhaka University (DU), Ministry of Education etc. did experience hacking or virus spreading problem within the academic and administrative Information devices. The culture of non-installation of antivirus and internet security or excessive use of USB flash drives led the named Institutions/organizations into dangerous IT security hazards. A known or unknown attempts to hack the results, grades, question papers, protected data are not unlikely when inexperienced and primitive IT culture are presented to the IT management system. The above mentioned cases showed the importance of a Robust IT security strategy, policy and environment in context of Bangladesh and specifically, in Higher Educational Institute.

From the point of view of developing country like Bangladesh which is emerging in IT sector exponentially must give due attention in securing its valuable Information. Universities and Higher Education Institutions are most vulnerable to give away large research related data that are done each year on a high number, confidential data related to question paper and answer for competitive examinations, seminar, symposium paper, related study materials and any worthy writings etc. can be very well exposed to unauthorized hand due to lack of strategy, less or no policy and practice. Though chances of damage or loss out of Hardware damage or theft may occur in some cases but the paper emphasized mainly on soft loss in context of Higher Education Institute of Bangladesh. Military Institute of Science and Technology (MIST) being a defense background and reputed Institute in Higher Education Sector must therefore concentrate in safeguarding its IT assets through robust strategy, policy and practice. For the reasons discussed above the study on MIST was undertaken to assess its IT security environment.

2.2.8 Recent Development of Information Security System Affecting Higher Educational Information Management System

Current IT development in Higher Educational Institutes of Bangladesh have almost at the frag end of Hard security measure. Though the development should have run side by side in the soft intervention of IT security but the reality is quite different. The strategy, policy and practice in connection with the hard intervention are still in evaluation stage which are also frequently changing. The volatile nature of the value and belief in relation to the common aspects of countering ever changing IT threats and vulnerabilities also acted as hindrance in devising and adopting a well-established. Long rehearsed IT policy and practice. The usual tools that are employed in hard methods include antivirus software, SSL for web transactions, centralized data backup, network firewall, enterprise directory, VPN for remote access, intrusion detection and prevention tools, encryption, content monitoring/-filtering, electronic signature, shibboleth and Kerberos. Normal trend suggest that Higher Education sectors appoint their Chief IT officer who basically ensures that the hard securities are completed as they are easy to install and visualize. Though some of the cases the organization might not agree to expense some extra money on not so imminent threat of IT security breech and compromise security [9]. Soft intervention on the other hand are not so easy to implement, while the development in IT sector is still in growing stage. Most of the budget are not been allocated for strategy devise, decision making. Policy making, standard operating policy generation, risk assessment, awareness program and management aspect. Normally everyone forgets that human are the weakest link in the IT security chain and gives least priority on human aspects of security planning. Therefore, considering the above scenario this paper suggest an assessment on IT security management system of one of the countrys reputed Institute namely MIST [9].

2.2.9 Major Focus of IT security Management System

In higher education, where much information used for teaching and research requires the highest level of integrity and availability but low level of confidentiality. Various research and national and international project work, paper, journal, thesis work, study requirements which are all of immense importance and must not be compromised resulting any security breech incidents. Soft interventions covering strategy, policy and practice are therefore the major concerns in relation to ensuring IT security in the higher education Institute. Most of the time the focuses tend to deviate from the above mentioned security approach and thus causing an insecure IT management system. The experts always put emphasize on constant monitoring and risk assessment of the management system that remains vulnerable in many cases from the culture of IT users. In case of an Educational Institute the tendency is more as because of its non-permanent nature of students and also faculty members. Some organization also tend to give IT responsibility with non IT certified personnel and semi or non-permanent personnel. The case study on MIST assessed the IT management system focusing its IT strategies, policies and practices that gives in-depth of information security status (strength and challenges) of MIST. Therefore, the study took a holistic view to focus only the cultural blend keeping in mind the major requirement of Information assets security.

2.2.10 Assess the Role of Soft and Hard IT Security Interventions on Higher Educational Information Management System

Hard Intervention uses security technology aggregation, when no a priori information about which types of security breach attempts may happen, the procedure consists in categorizing the security incidents into a unified pattern according to a similarity criterion, where the selection of the similarity criteria depends on the pattern and types of intrusions that already occurred in the field of education or i.e. on the problem under consideration. Several examples where this method has been applied can be found in ”Identity management in higher education: A baseline study” [3]. Security collaboration grows by appending the functionality of each tool of Hard intervention with that of the next tools having specified security properties in a sense to smoothen the system execution, intrusion detection and prevention, client secrecy preservation and thereby client comfort maximization.

Security balancing by soft interventions is just opposite to the hard one. It largely vary with that of the cultural aspects i.e., policy, organization, leadership, awareness and practicing structure of a particular institution. Where, the association of these soft aspects with the ongoing campus security process is governed by a value criterion that must be satisfied in order to implement this framework around the arena. The value criterion is academia dependent and may be dynamic within a given academia. But in general this largely focus

on the preservation of academias values i.e., freedom and openness and academias believes. If any of these soft features contradicts with the values criterion should be reviewed and revised but should not be purged, where a compromise in any one of these issues may cause a total loss. This procedure continues until each of these cultural aspects fully relay with the defined value criterion of an academia and should not be a conclusive one because of the transient nature of the academias constitution and rapid changing nature of the intrusions and technologies. The main drawback of this method is that it is very hard to make people believe that we are not Employer rather the colleagues and solutions may not be a global one as well as time lag between deployment of technology and the development of legal and policy framework for its appropriate use can also hinder the security outcomes [18].

2.2.11 Propositional Structure of Soft and Hard IT Security Interventions on Higher Educational Information Management System

To enhance the performance of the security balancing process and to address the drawbacks of only having the hard with the light of the concept of the soft security patterns as discussed above, this section presents a newly developed security balancing scheme called Robust IT Security Balancing (RITS-B) approach [9]. Based on the use of the technological and cultural aspects Kavavik & Voloudakis have suggested four major strategies or approaches Figure 2.2 for securing an educational institution on the basis of the institutions strength in each arena [5]. Information technology security: Governance, strategy, and practice in higher education, ECAR Study of Undergraduate Students and Information Technology, 2013. Louisville: Educause,2013.

The proposed RITS-B approach contains six main constituent parts which are applied on the institutions hard layout with that of the scale to assess and scope to apply and improve and are: (i) Management structure of IT security, (ii) Organizational Structure of security (iii) Policies and plans (iv) Communication and awareness (v) Security practice pattern and (vi) Security end user use scheme. In this RITS-B approach information security balancing process is summarized into four (04) stages: Identification-Prioritization-Revision-Dynamicity. (1) Identification- Identify the exiting higher education environment. (2) Prioritization- Prioritize the IT security issues around the academia and administrative arena of that environment. (3) Revision- Revise instructional security governance, strategies and practices and improve the use of existing security tools and (4) Dynamicity- Keep the paces with the educational and environmental changes rather being to be conclusive.

The three main constituent parts of this RITS-B approach is: (a) definition of the scope of information security in that particular school arena (b) having a look on what types of security tools academia is currently installing (c) and then try to determine a soft layout on them to know how best to practice, when to practice, by whom and at what level, how and

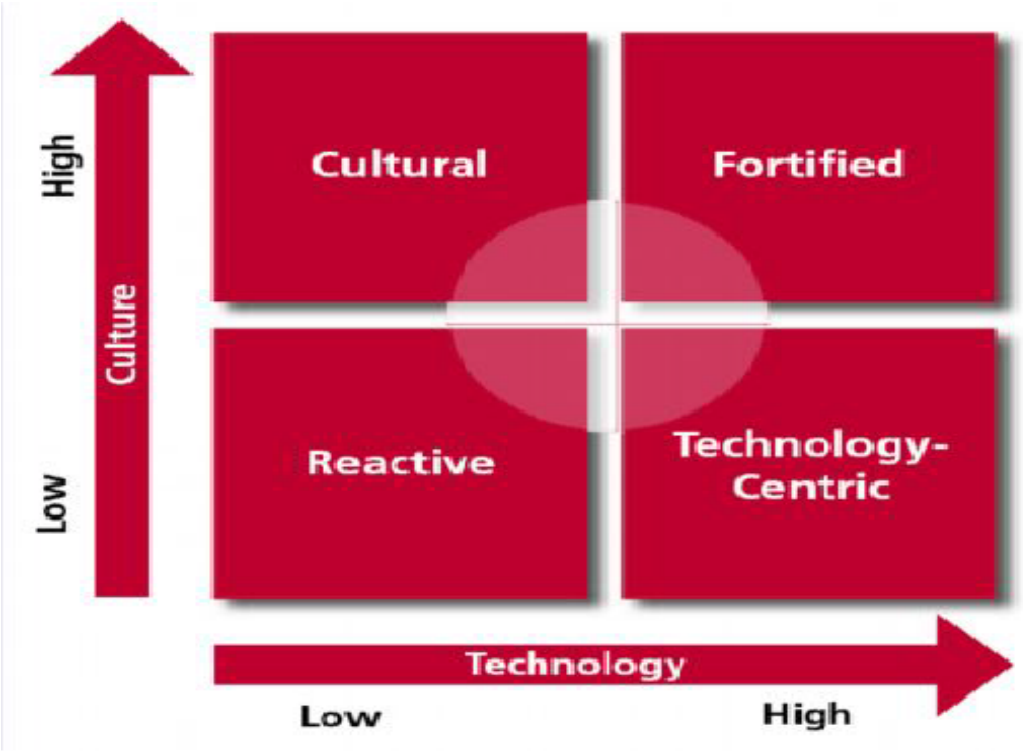

Figure 2.1: IT Security Approach

what to aware, how to cope up with the incidents i.e., in a single word how to merge the institutions cultural layout with that of its existing hard framework to satisfy the following requirements: (a) Technology i.e. security tools (b) Policies (c) Awareness (d) Leadership (e) Practices and (f) Academias values and believes which has produced the requirements of these fives and other consequent security requirements generated by these ethical concerns. Kvavik & Voloudakis have suggested the following risk assessment methodology Figure 2.2 which is capable to address the different IT risk [5, 15].

2.2.12 Economic Crises Those Could Lead Higher Education Sector Towards Adoption of A Robust IT Security Management System

It is very difficult to identify what exact enterprise security processes or technological tools are needed for strengthen the IT security infrastructure around the campus arena of higher education because tools are dynamic in nature and depends on the application area and types of breaches. For this reason, one tool is appropriate for execution of one type of application or the identification of one type of intrusion while may not be suitable for other applications and intrusions and this raise an open question which sets of technical aspects are suitable for which type of application and intrusion? Section I depicts some of these common used tools. However, among these technical tools few are chosen optimally to from the standards for application and system development. Different higher education IT security approaches

Figure 2.2: Risk Assessment and Response

use different set of tools. The ultimate goal is to fulfill the requirements of (1) to (9) of sub-sub-section 2.2.9. In the same way economic crisis can also lead to the ultimate goal of IT security issues (requirements of (1) to (9) of sub-sub-section 2.2.9.) to be fulfilled thus requiring RITS-B approach to be adopted. Those crises could be as many as the following:

- Information technology security administrators should expect to devote approximately one-third of their time addressing technical aspects. The remaining two-thirds should be spent developing policies and procedures, performing security reviews and analyzing risk, addressing contingency planning and promoting security awareness;
- Contain and reduce costs: The bleak economic outlook and reduced funding sources are making it imperative to reduce or at the very least contain the growth of costs. Efficiencies are sought, and business best practices are often viewed as the best path to achieving efficiencies.
- Meet students' and faculty members' expectations of contemporary consumer technologies and communications: Students and faculty not only expect that they will be able to use their smartphones, tablets, and consumer-based apps in their academic work but also expect that their institutions' services will work as elegantly and effectively as commercial services.
- Disruption, transformation, opportunity, or simply change, the impact on IT depart-

ments and staff is enormous. IT organizations are scrambling to devise new strategies for security and support in response to explosive uses of data and consumerism of information technology.

- The degree of security depends on three factors: the risk you are willing to take, the functionality of the system and the costs you are prepared to pay;
- Lack of resources, change in global economy and budgetary constraint lead to change in policy.
- Reshaping of organizations value and belief resulting from economic crises: These has enormous and long term effect on all IT staffs and setup policies that might lead to an obvious drastic change to RITS-B approach.

2.2.13 Impact Analysis of IT Security Management System on the Predicted Information Security Trends and Developments in Higher Educational Information Management System

IT Security Management System (ISMS) is an example of applying the management system conceptual model to the discipline of Information Security. An extensible framework from which to manage information security compliance is the main aspect that perfectly match the required strategy, policy and practice of MIST. An ISMS is typically risk based, and process oriented. There may be multiple layers of abstraction to accommodate the distinct audiences whose concerns must be addressed. The ISO 27001 standard recommends a Plan-Do-Check-Act (PDCA) process-based approach. Establish the ISMS. The users must be made to understand the secured information usage management system. The Organization/Institute risk has to be managed and Information security program to be chartered. The authority has to assess the program risk by Implementing and operating the ISMS so that nobody can breach the data security management system. The governing body has to create the information security baseline of MIST and to create domain specific implementations. Monitoring and review of the ISMS is also done properly. Assessment of operational risk, maintenance and improvement of the ISMS is part of strategic plan.

Hence, the management system of Higher education is purely secured in an IT Security Management System (ISMS). The Unauthorized Disclosure of information to individuals not authorized to view such data continues to be the leading type of information security incident that colleges and universities suffer [18]. The IT security management system is rapidly changing, and may bring significant change [4] in regards to the use of ISMS successfully as follows:

Tools available to manage IT security are rapidly becoming more available and more ca-

pable, as are the tools available to hackers. The legal management system surrounding IT security is becoming more complex, presenting both challenges and opportunities. Automated attacks are replacing individual hackers thus becoming the most likely cause of a security breach. Institutions will come under increased pressure from their constituents to provide robust IT security, as its profile rises. The changing nature of threats and the increasing sophistication needed to combat them may prompt a move to more centralized and standardized management of security at large institutions. Many institutions, particularly smaller ones, may seek assistance from consortia or vendors in managing the increasing burden of IT security management.

2.3 Organizational Profile: MIST

Military Institute of Science and Technology (MIST), the pioneer Technical Institute of Armed Forces, started its journey from 19 April 1998. It operates several undergraduate and graduate programs in various disciplines of engineering for both military and civil (male and female) students. Since its establishment, MIST had six engineering disciplines, namely Department of Civil Engineering (CE), Department of Computer Science & Engineering (CSE), Department of Electrical Electronic and Communication (EECE), Department of Aeronautical Engineering (AE) and Department of Naval Architecture and Marine Engineering (NAME). The institute is launching four new departments from the academic session 2014-2015.These are Department of Nuclear Science & Engineering (NSE), Department of Architecture (Arc), Department of Environmental, Water Resources & Coastal Engineering (EWCE) and Department of Biomedical Engineering (BE). MIST is located at Mirpur Cantonment, which is on the northwest of Dhaka City. MIST is a hub of knowledge for military and civil students and its vision is to become a Centre of Excellence. So far four departments of MIST namely CE, EECE, ME and CSE have achieved accreditation from Board of Accreditation for Engineering and Technical Education (BAETE) which is certainly considered to be a pronounced achievement for its academic excellence in national and international arena.

First Academic Program at MIST was launched on 31 January 1999 with the maiden batch of Civil Engineering (CE). Computer Science & Engineering (CSE) Program got underway from academic session 2000-2001. Presently students from Srilanka, Maldives, Palestine and Afghanistan are also studying different Engineering Programs in five Engineering Departments. MIST enters into the domain of Online Admission System since 06 Sep 2010.MIST has well equipped class rooms with multimedia and web camera with internet facilities and Laboratories with modern equipment. All academic programs of MIST are affiliated with the Bangladesh University of Professionals (BUP) and have close cooperation with Bangladesh University of Engineering and Technology (BUET) and Dhaka Univer-

sity (DU). MIST has other miscellaneous facilities such as Medical Centre, Fitness Centre, Cyber Cafe, Broadband Internet facilities, Library and Students Accommodation (Male & Female).

MIST conducts a number of sponsored research in each academic year and operates several major research labs like Microprocessor and Micro Controller Lab, Artificial Intelligence/VLSI Lab, Software Engineering Lab etc. There is a dedicated Research & Development Wing for research in MIST. At present around 150 faculty members and 1500 students are contributing and pursuing various Higher education courses respectively. Therefore, IT dependency of MIST in multidimensional and prospective study, research, project work etc. generates a definite requirement for the study on IT security management system. MIST IT budget distribution are shown approximately for year 2013-2014, for IT security purpose around 4,50,000 taka was expended,besides this, device security purchases crossed around 10,00,000.MIST did install and updated their server facilities in last fiscal year with an expenditute of 1 Crore Taka exclusively.

2.4 Critical Assessment

The university or Higher Education Institute is under tremendous challenge of IT security threat at present era. This case study highlighted on important aspect and elaborated major concerns because of the IT security environmental reality that it took into consideration: Wireless systems present new avenues of attack for potential hackers. While MIST does require MAC address registry for network use, there is concern that someone could surreptitiously join the network and perform undesirable activities, such as sending spam. Vendors dont necessarily incorporate security in a usable way. Most vendors assume that users run their security applications behind a firewall or use a virtual private network (VPN). Most cant handle single sign-on or encrypted applications. The difficulty in quantifying the value of security makes it difficult to convince senior management to invest in security. The difficulty of justifying additional security resources during lean fiscal times might be a related issue. The number of attacks continues to rise monthly and the monthly attacks are likely to triple within a year. The nature of these attacks is also changing: more are automated. Automated worms pose particular problems because they exploit vulnerable machines in a matter of hours, requiring more manpower to respond more rapidly. Restricted information access fosters illegally stored data on desktops. People ask those with data access to run reports off the data ware-house, creating new files on staff members desktops. The problem is how to loosen access without compromising security. Lack of data ownership standards also impacts Roles. When authorization was paper based, the requestresponse paradigm worked pretty well, but it does not scale well into the electronic space. Response time decreased significantly. With faster machines and faster networks, the security team will have

less time to respond and must therefore find ways to react faster. Speed of communication and access had improved. Hence Preparation for the future is an important consideration. Thinking about what kinds of things could strike the universitys network and testing rapid response capabilities give a proactive upper hand. The unthinkable is now potentially a daily reality with root causes of information breaching, misusing and thereby initiating terrorism which have presented the world with many challenges in accommodating peoples personal and work lives to a changed environment. To bring the resources of the academic world to bear on both national policy and on the individual responses and so thus to cope up with and to mitigate such riskier environment various IT security approaches have been proposed. While among them Soft IT Security approach (SITS) is highly lucrative now-a-days due to its simplicity and effectiveness in the sector of Information security especially in higher education, it is unable to secure the all types of educational environment using a general framework due to not most of these environments being homogeneous also because of little focused on cultures and believes.

Addressing this issue, a new security management scheme namely Robust IT Security Balancing (RITS-B) Approach is proposed which is focused on to develop such strategic framework of security environment where facts, national and regional perspectives will be merged up to lead to a proactive leadership and information security system without violating the freedom and openness that is at the very heart of the academia. MIST being the case study, an assessment its IT security environment gave the in-depth of the strategy, policy and practice that are adopted by MIST to secure organizations information assets. The analyzed data helped us to assess the IT security environment state in line with our proposal and to present necessary corrective measures which were in the form of recommendation.

2.5 Identified Knowledge Gaps

This study has identified that human is the weakest link in IT security measures taken so far. Previous all study showed that firewalls and policies that were in vogue and research on them gave mixed feedback while rate of failure remained alarming. Herby a general outcome tend to lead a mixed but balanced approach that might working all possible dynamism and changed management system. No concrete decision though could be made on any solution to IT security management system, we tend to grow our interest on an integrated approach where management knowledge is blended in IT management system. Moreover Higher Education Institute being largely exposed towards the security breech incident in recent past, needed an extra attention as they have larger IT/user network. Inculcating the two aspects in one gave us the scope to assess the IT security management system of such Institution that has IT based learning and growth for its user rapidly. So, we could successfully identify that a scope remained in terms of case study on such Higher Educational Institute to assess

its IT security management system and identify required improvement facilities in terms of theoretical IT security measure. ISMS and RITS-B could be the assessment scale that could help defining, suggesting and measuring organizational model and at the end an easy to use scheme could be developed for awareness purpose. A case study on MIST was therefore finalized to assess IT management system.

2.6 Analyzing the Original Research Questions and Research Objectives with Respect of Theoretical Framework of References

It reflects the assessment on perceived use of IT resources and information assets management through strategy, policy and practice which the case study aimed to be measured on its usefulness, ease to use, credibility, intention and adoption those formed the IT security management system for MIST. Three factors are found to be characterizing the organizational performance of IT management system: (a) its strategy (b) Policy for long and short term and (c) Practice (cultural) aspects. For this study the factors are evaluated and assessed in details to measure the impact of it on IT performance of MIST, when hard security intervention is merely defined to be easy but not favorable in Higher Education Institute e.g. MIST [9]. It was rather encouraged that the Organization should establish a robust IT security balance in protecting their IT resources and assets. Because retaining satisfied IT user at the present era of IT security where activities vs. counter activities are the base of sound, effective and popular IT culture that necessarily endeavors well-laid policy and awareness of each responsible personnel. The case study not only identified the present IT management system of MIST but also directed a risk audit, easy to use scheme for users to aware themselves and check listing security measures on regular basis. Thereby the study succeeded to provide a security guideline for upgrading to a more secured IT management system in Higher education Institutes.

2.7 Summary

The simplest security model is to describe each aspect of institution by their respective security management structures. Higher education institutions should designate an individual to be responsible for IT security and these key responsible personnel should report to their respective senior management and should bare a certain level of security certification. Even though certification dont prove knowledge but shows that you putted your time and effort to gain the specialized skill The salary trends of these IT security personnel are further queried It is very difficult to identify what exact enterprise security processes or technological tools are needed for strengthen the IT security infrastructure around the campus arena of higher

education because tools are dynamic in nature and depends on the application area and types of breaches. For this reason, one tool is appropriate for execution of one type of application or the identification of one type of intrusion while may not be suitable for other applications and intrusions and this raise an open question which sets of technical aspects are suitable for which type of application and intrusion? Section 1 depicted some of these common used tools. However, among these technical tools few are chosen optimally to form the standards for application and system development. Different higher education IT security approaches use different set of tools.

CHAPTER 3
RESEARCH METHODOLOGY

It is necessary for a researcher to design a methodology for the problem chosen. Even if the method considered in two problems are same, but the methodology may be different. It is important for the researcher to know not only the research methods necessary for the research under taken but also the methodology. To find out the best output from a study the researcher needs to sort out the suitability, efficiency and order of accuracy of a chosen research method. There must be a clear understanding about how to find a solution of a physical system described by mathematical model and how to apply a particular method as suited to the problem.When the research has been completed,there must an explanation of the used methodology so that others can understand the significance of the research and how itworked.It also enables the researcher to express about each of the actions conducted and the possible causes behind it, and about the limitations of the research as well as its strengths. The information incorporated in this report has been collected both from primary sources and secondary sources. The information has been used in the subsequent levels to find up the facts that are prevailing in the information security management system in the focused research area.

3.1 Research Design

The research has been conducted based on two approaches- quantitative and qualitative. Quantitative research process has been used to collect the data.Quantitative Research focuses more in counting and classifying features and constructing statistical models and figures to explain what is observed.It is used to quantify the problem by way of generating numerical data or data that can be transformed into useable statistics. It is used to quantify attitudes, opinions, behaviors, and other defined variables and generalize results from a larger sample population. Quantitative Research uses measurable data to formulate facts and uncover patterns in research. Quantitative data collection methods are much more structured than Qualitative data collection methods. It include various forms of surveys online surveys, newspaper surveys,mobile surveys and kiosk surveys, face-to-face interviews, telephone interviews, longitudinal studies, website interceptors, online polls, and systematic observations. Qualitative Research is primarily exploratory research. The primary aim of a

Qualitative Research is to provide a complete, detailed description of the research topic. It is used to gain an understanding of underlying reasons, opinions, and motivations. It provides insights into the problem or helps to develop ideas or hypotheses for potential quantitative research. It is also used to uncover trends in thought and opinions, and dive deeper into the problem. Qualitative data collection methods vary using unstructured or semi-structured techniques. Some common methods include focus groups (group discussions), individual interviews, and participation/observations. The sample size is typically small, and respondents are selected to fulfill a given quota.

3.2 Research Paradigms

The research paradigm can be called as the philosophy where choice of this paradigm largely depends on researchers personal thinking and believes to choose which way to go and how to conduct the intended research where every paradigm is true on the ground of the intended task .According to Taylor, Kermode, and Roberts [19] ,a paradigm is a broad view or perspective of something. Thomas Kuhn who is known for the term paradigm, characterizes a paradigm as: An integrated cluster of substantive concepts, variables and problems attached with corresponding methodological approaches and tools. It is necessary for the researcher to understand the philosophical position of research issues to understand the different combination of research methods.

There are mainly three type of paradigm to understand the reality- (1) Positivism: The positivist paradigm of exploring social reality is based on the philosophical ideas of Aristotle, Emmanuel Kant and August Comte [20]. It is also known as the science research or scientific method. This approach emphasizes observation and reason as means of understanding human behavior. According to this paradigm, researchers are interested to collect general information and data from a large social sample instead of focusing details of research. Researchers own beliefs have no value to influence the research study. The knowledge is based on experience of senses and can be obtained by observation and experiment. Positivistic thinkers adopt his scientific method as a means of knowledge generation. With the assumptions and acquired knowledge the ultimate goal is to integrate and systematic findings into a meaningful pattern or theory which is regarded as tentative and not the ultimate truth. Positivistic paradigm has influenced the educational research in the last half of the twentieth century. It regards human behavior as controlled and determined by external management system. Hence human beings are driven without their intention, individualism and freedom taken into account in viewing and interpreting social reality. (2) Interpretivism: It can be referred as the Social Constructionism in the field of management research. With the help of this philosophical, researchers focus to highlight the real facts and figures according to the research problem. This kind of philosophical approach understand specific business sit-

uation. In this approach, researchers use small sample and evaluate them in detail [21]. (3) Realism: This research philosophy mainly concentrates in the reality and beliefs that are already exist in the management system. Direct reality means, what an individual feels, see, hear, etc. On the other hand, in critical realism, individuals argue about their experiences for a particular situation [22]. This is associated with the situation of social constructivism, because individual tries to prove his beliefs and values.

In this research both the positivism and realism approach has been used. These approaches are very popular for conducting a research like this one. Though there are many more modern approaches are available nowadays but the progressive research specialists still have their faith to on them. Because these approaches are very convenient for any kind of environment and has the ultimate ability to suit in any major field of technology and social sciences. Also they are very cost effective which gives the researchers a positive edge. This research had not enough time constraint or budget to interview all the concerned users . The researchers had to conduct an interview with a group of concerned people. That is the process which enables to collect data and information from a convenient social arena. Thus this approach leads the researchers to positivism.

3.3 Research Strategy

According to Dahler-Larsen there could have been fourteen different strategies to be adopted for the conduction of a particular researcher [23]. But this study has adopted a qualitative approach in the form of face-to-face interview which incorporates an inductive strategy with the content analysis theme to have the in depths of the every aspects of this particular research. This qualitative approach mainly deals with the Subjective data where different methodologies are used in this approach for analyzing the data as further stated [24]. According to him, its a kind of approach which typical focuses on the past art factual data in the form of observation note, tapes, interview transcript, focus group findings to have the in depths of a particular research setting. In this research the actual findings have been focused in the satisfaction of the users from the level of service, the drawbacks of the system and the possible and proposed scope of development opportunities in the existing infrastructure.

3.4 Population of the Study

For this particular research work the students, faculty members, the IT stuffs of MIST can act as the population for this intended study. But to avoid any complexity and procrastination only 50 students from the five departments were selected for the work. The students were divided into 2 basic categories referred as residential and non-residential. All the de-

partments and all the four levels have been covered to collect the most precise review of the IT management system and facility they are enjoying here. To cover the faculties, all the members including the Head of the Department of the Department of Computer Science and Engineering have been interviewed. Later on the reviews from the selected members of the other faculties of the other departments were taken. A very important part of this research was the opinion of the IT persons and that was emphasized thereby. All the persons from different category faced different sets of questionnaire with a little similarities which were not much to make a big difference in the final findings of the research.

3.5 Sampling Strategy

Data sampling is a statistical analysis technique used to select, manipulate and analyse a representative subset of data points in order to identify patterns and trends in the data set being examined as a whole. Sampling allows scientists, predictive modellers and other data analysts to work with a small, manageable amount of data in order to build and run analytical models more quickly, while still producing accurate findings. To find the facts and to analyse the responses of the interviewed persons the recorded data should be sampled in a scientific manner so that we can visualize the exact scenario that can lead the researchers to focus on the security holes. For this particular research work the students and IT stuffs working at MIST will be considers as the sample where 50 students will be surveyed as the primary data source where the selection of sample size will be done on Convenient sampling methodology which is easy and reachable within the predefined time, and also respondents have the specific know-how.

The primary positive aspects of this sampling strategy is that it will allow us to access the samples within a convenient time where the focus group will also help us to have the in depths which will further help us to logistically analyze the study variables and correlate them accordingly to reach to a rich conclusion. The primary negative aspects is that because of convenient sampling the responses that we will get might not represent the perception of the different user group which could be gathered if stratified sampling were in use and thereby could further act as a paradox in generalizing the actual study findings. Also the fact finding from all the samples would consume a huge amount of time which will lead to a setback.

3.6 Data Collection

There are four data collection incentives that incorporate in this particular research work and these are: (a) Secondary elements i.e. the literature review, internet references for similar re-

search on different educational institutions or commercial organizationshas been evaluated logistically to figure out the major study elements and variables. (b) Consultation has been done with the supervisor and the researchers of the research group by the researcher himself to find out the logistic research elements and factors to be evaluated and emphasized more which thereby make it easier to set the layout of the research questionnaire. (c) 50 MIST students has been chosen on the basis of the convenient sampling methodology were interviewed face-to-face by the researchers with a period of 10-15 minutes per person covering a set of appropriate questionnaire to have the in depths on their concerns and opinions regarding the factors impacting their use of the internet facility and information managament system. (d) 20 faculty members from all the major departments including CSE department were interviewed face-to-face for data collection also. They faced a different set of questionnaire because they have to maintain a different protocol from students and IT persons. The primary positive aspects of these data collection techniques are that it will help us to have the in depth facts of the factors that are prevailing in the field of information security and how the system will respond in an event of data security incident. Moreover, the critical literature review and the consultation made with the experts will further help us to logistically set the every aspect of the survey instruments to explicitly identify the study factors. However, the primary negative aspect of this is that the lengthiness of the process and if the interviewer is not expert enough to deal with this focus group and to deal with this face to face interview session the exact study concerns will not come out.

3.7 Data Analysis

A quantitative and qualitative approach were used for the analysis of the collected data. And these data collected through the face-to-face interview will be analyzed on inductive thought with the use of content analysis approach while inductive thought refer to analyze a particular setting on a multiple truth where single truth would be insufficient to lead towards a more realistic conclusion. And all necessary secondary information will also be incorporate to strengthen the data support. The primary positive aspects of this data analysis technique is that it will help us to have the in depths of the study as the data will be analyzed on multiple truth using inductive approach. But the primary negative aspect or the major drawback is that only analyzing the study findings qualitatively might not represent the exact outcomes as while interviewing the interviewee might be unaware of some aspects which a quantitative question might help him/her to recall and thus will further strengthen the study support. Moreover, this qualitative analysis will further restrict us to check the significant impact of some variables as the significance could only be analyzed using statistics.

3.8 Limitation

The kind of research that has been conducted always has to be under that complete sieve of the authority, any kind of information needed cannot be fetched without their proper concern. So it is not always independent, which may hinder the way to find the real facts of the intended survey. Only those persons were inquired who poses enthusiasm to participate and reflects their thinking on this research theme whether other demotivated people could act as a great option to find out the more details and research factors. But only a handful of member of such a large community or user group cannot always reflect the philosophy, motivation or expectations as a whole. Moreover, with the predefined time constraints it was not possible to access the most confidential organizational information which might be useful for analysis those internal factors. In addition to it, this research begins with an assumption that the responses are done knowingly and correct and without having any kinds of biasing but if not it could make the whole research strategy vulnerable to any kind of integrity theft and could act as a great barrier to its robust acceptance. The ignorance or negligence of the interviewee may create a hazardous result. The data that have been obtained could be proven valuable to assess the assumed correlation and to establish the links. Only a fair and accurate result could be found if all of those hindrance could be eradicated as a precaution.

3.9 Ethical Consideration

This particular research work consent has been taken a prior from the respective authority of MIST to access their faculty, IT employees and students. Moreover, this study has tried to ensure the willing participation of students and stuffs without having being forced them or provoking them to do so. All the students, instructors and the stuffs were accessed for interview from the direct permission of the concerned authority. In addition to it, the objective and the intension of this research along with what will happen to the collected data and how will they be managed was details a prior to the participants to enable their comfort in the participation. Further to ensure the data confidentiality this study avoids to utilize any permanent database for information storage and any analysis strategy that would possible lead the data with the responding personal utile having the permission for them for retention. However, this study avoids defining any further information and data i.e. location of covert research or any other specific characteristics that would link to the study sample either directly or through cross-referencing. However, the databases which were used either for temporary or permanent data storing were safe enough for preserving data confidentiality.

3.10 Linking Sampling strategy, data collection and data analysis technique with the Research Questions

The sampling strategies that have been chosen, the data collection and data analysis technique that has been used further support the logistically outline this research question. As the prime focus is on the preparation of the information security system on the event of a security threat, a face-to face interview with the IT employees will help us to have the in depths on these factors. While the consultation with a selected group of students a prior along with reviewing the secondary study elements i.e. literature review will further help to identify the major study elements and a line the interview layout accordingly on which to be focused and which will not be. Furthermore, the inductive analysis technique will further assist the research question by ensuring the perfect correlation of the security factors and user intention to work in the organization. Thereby after the data have been found, they are analyzed according to the selected approach and the results will be generated. Discussing the results, the decision will be taken.

CHAPTER 4
RESULT, ANALYSIS AND DISCUSSION

This analysis part explores the information technology security strategy, policy and practice used in MIST through the case study. What policy have they chosen to adopt, to prevent harm to their information assets? Do the institution deviates from standard practice in these perspectives? For example, do they practice ISMS purely to implement IT security strategies in an organized manner? Or, do IT security awareness program or risk assessment analysis is of top priority in MIST? Technologies discussed here defined by functionality, scope of use, objectives and the threats they address reviewed from users perspective.

4.1 Qualitative Results

A qualitative analysis through the interview with Hossain, Md. Azmal, Chief IT and Maintenance Officer at Military Institute of Science and Technology (MIST) gave an in-depth of IT management system converting in an interpretative, impressionistic manner or diagnostic. The qualitative approach was used to gain an understanding of underlying reasons and motivations and to uncover prevalent trends in strategy, policy and practice of the present IT security management system of MIST. The respondent gave a detail view from point of view of human behavior, practice and policy. The findings that were brought are presented sequentially.

4.1.1 General

MIST has an official in charge of IT cell whose appointment is known as OIC IT cell. Institutional network could connect approximately 1001-2000 devices whereas serving nearly 501-1000 user. The Institute use a third-party service provider (SP) for net facility and dont have an on-site data center server. MIST does not provide remote network access/VPN/-Campus modem pool/outsourced modem pool.

4.1.2 Staffing

MIST has a well-established IT cell to manage IT facilities within the campus and residential members of MIST. Network administrator who is CCNA certified personnel manages the day-to-day IT security in fulltime basis and report incident handling to IT OIC immediately.IT OIC form an important part in developing and adopting strategic and operational aspects of IT in MIST. Strategy covers both short and midterm vision at present focusing a long term security to be undertaken in near future. The infrastructure of IT security is underway and taking a holistic effort in day to come.IT cell runs with dedicated professional experts(more than five) who are qualified in IT and given responsibilities that are spread across multiple functions. (*see* Appendix B)

4.1.3 Policy

MIST has formal and well-practiced IT security policy monitored and updated regularly which was in vogue since last at least five years or more. The policy adopted covers appropriate use of institutional IT assets, enforcement of institutional security policies, desktop security(anti-viruses etc.), system access control(password management, authorization, authentication, data access, privilege management, physical security of IT assets, network security(firewalls etc.), resident halls, remote devices and authority to shut-off internet access.

The respondent strongly agreed that MIST has a comprehensive, regularly updated, consistent and easy to read IT security policy where respected Dean of MIST, Head of the department of Computer Science and Engineering (CSE) and OIC IT cell were actively involved to input their thoughts. (*see* Appendix B)

4.1.4 Current IT Management System

According to the respondent its obviously the IT security that forms an integral part of strategic plans of MIST which is at present undergoing strict scrutiny, validation and approval to be implemented as soon as possible.IT security approaches which are under consideration and implementation in process are (a) Centralized data backup system (b) Secure Socket Layer (SSL) (c) Intrusion detection (d) Intrusion prevention tools (e) active content monitoring/filtering. Institute provides MAC address authentication system for wireless technology that is available for students and stuffs. (*see* Appendix B)

4.1.5 Awareness

The respondent strongly agreed that IT security is one of the top three IT issues that MIST is confronting today. He also agreed that IT security problems inadvertently caused by an authorized user are also a significant concern for the Institute. The respondent added, Our Institute aware students, faculties and staffs about IT security and how best they can act securely in modern days IT threat and vulnerabilities, which I do agree is effective for all concerned.IT security organization often reports to senior management on IT security in MIST. (*see* Appendix B)

4.1.6 Enterprise Process

MIST at present are not planning for single sign on system but using multiple use passwords while smart card based authentication is also under consideration. Institute is planning to have an Institute wide password policy to be devised. As per the respondent, there are daily monitoring of networks, operating systems for vulnerabilities and attempts at unauthorized access. They use email, application from the third-party and web, FTP and database server. MIST has licensed anti-virus installed devices for servers and operating systems. But its non-mandatory for any institutionally or non-institutionally owned system to have anti-virus installed. Currently, MIST doesnt cover licensed anti-virus for personally owned system. The respondent informed us that limiting the types of protocols allowed through firewall/router, limiting the URLs allowed through firewall/router and restricting and eliminating access to servers and application are already implemented to reduce IT security vulnerability. Timing out access to specific application, using security devices(cards, biometric scanners etc.) for personal authentication and Instituting a recovery or back up plan in the case of disasters caused by natural events or by human acts are the enterprise processes under consideration to implement for reducing IT security threat and vulnerabilities. (*see* Appendix B)

4.1.7 Incident Handling

An IT security incident can be assessed by some aspect of IT security that could be or has been threatened e.g. loss of data confidentiality, disruption of data or system integrity or disruption or denial of availability. The respondent further noted, IT security incidents were reported to higher officials/personnel concerned on as and when basis (i.e. when incident happens).We have a centralized mechanism to alert faculty/staff/students on IT security incident handling procedure. (*see* Appendix B)

4.1.8 Risk Assessment

The respondent mentioned, MIST did not undertake formal risk assessment to quantify the value of their IT assets and risk to those assets but they did perform IT security review and vulnerability assessments on quarterly basis. He further noted, MIST locally conduct weekly basis assessment on integrity of data and unauthorized changes made to it. And in case of router configuration, it is daily. Review of dormant or invalid account activity is made weekly while access control review is on a monthly routine. MIST being a Military run Institute the criminal background of all related employees who have access to IT asset is always checked strictly and judiciously(default action), even those contractors involved directly or indirectly in the key enterprise process of MIST are security cleared. MIST have not outsourced any IT security consultants in last one year. (*see* Appendix B)

4.1.9 Funding and Budget

According to the respondent, MIST had used very minor portion of its total budget dedicatedly for IT security management system (Secured internet facility and data sharing, security awareness briefing/address, infrastructure development etc.) in last one year. However, he did expect some increase in staffing, hardware/software/products and education/training in upcoming year. (*see* Appendix B)

4.1.10 Outcomes

The respondent evaluated the IT security programs as fairly successful for MIST. He opined that data, network and applications within his jurisdiction are secured and a more secured IT management system is prevailing than it was at least four years back. (*see* Appendix B)

4.1.11 Future Directions

Lastly, the respondent evaluated top three major barriers to IT security at MIST are to be-(a) Resources (b) Awareness (c) Time lag between deployment of technology and the development of legal and policy framework for its appropriate use. He disagreed with the statement that MIST IT security architecture and implementation sacrifices some level of protection to ensure ease of use. (*see* Appendix B)

4.2 Quantitative Result

Followed by qualitative research which are used to explore further findings on IT security management system of MIST, quantitative research on students and faculty were carried out. Structured questionnaires were used to get the responses from randomly selected sample representatives of the larger groups. Statistical data was drawn which were further analyzed for the conversion of conclusive findings. Final outcomes are naturally in the descriptive type which supplements the recommendation for future course of action.

4.2.1 Existence of IT security policy

All the data collected were analyzed using Statistical Package for the Social Sciences (SPSS) and used after processing for comparison and discussion under various IT security environment issues. Table 4.1 (*see* Table A.4 Appendix-A) shows the data obtained on the question that were asked to faculty members of various departments of MIST. Not surprisingly (forty-five) 45% agreed that IT policy of MIST is clear and easy to read type, while (twenty) 20% did not have any clue about the policy. On the contrary, (twenty-five) 25% and (ten) 10% disagreed and strongly disagreed respectively with the statement that might indicate lack of effort in dissemination of the policy and awareness measures.

Table 4.1: IT Security Policy Patten

My institutions has IT security policies that are clear and easy to read(faculty)	Response on IT Security Policy Patten (N=20), (Frequency(Percentage of Respondents))						
	SA	A	DA	SD	DN	WA	S.Dev
	-	9, (45%)	5, (25%)	2, (10%)	4, (20%)	3.05	1.191
Scale:1(Strongly Agree) = SA, 2(Agree) = A, 3(Disagree) = D, 4(Strongly,Disagree) = SD, 5(Dont Know) =DN. N=20 (faculty), WA= Weighted Average.,S.Dev. = Standard Deviation.							

4.2.2 Existence of IT Security Practice

Not so expectedly (sixty-five) 65% faculty members did answer negatively while they were asked whether or not they were provided with a confidential digital repository for classified materials to store in MIST (*see* Figure 4.1 , Source:Appendix A.1).

4.2.3 Concern of IT security Awareness Issues

The data analyzed in SPSS were tabulated for comparison. Following the process Table 4.2 (*see* Table A.5 Appendix-A) Table 4-2 showed that more than (thirty) 30% of residential

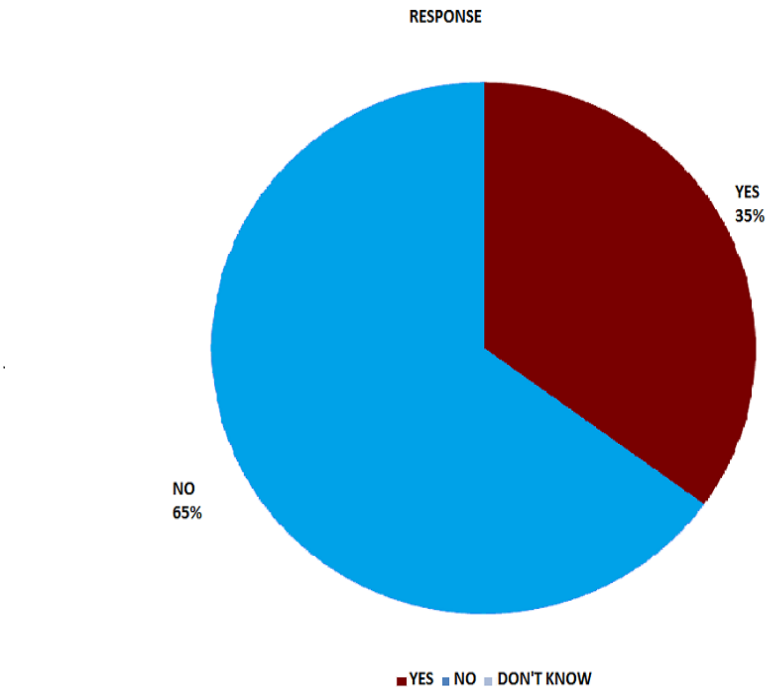

Figure 4.1: Response on Existence of IT Security Practices (N=20)

and non-residential student agreed about the fact that MIST communicates awareness issues regarding IT security with students. While disagreed students were more, (forty-five) 45% and (forty-three) 43.4% respectively for Non-residential and residential students respectively. A significant number of student did reply indefinitely and stood neutral (15%and 26.7%respectively).

Table 4.2: IT Security Awareness Patten

My institution communicates IT security,awareness issues for its students (student-Nonresidential and Residential)	Response,on IT Security Policy Patten (N=20),(Frequency(Percentage,of Respondents))						
	SA	A	DA	SD	DN	WA	S.Dev
	2, (10%)	6, (30%)	6, (30%)	3, (15%)	3, (15%)	2.95	1.234
	-	9, (30%)	8, (26.7%)	5, (16.7%)	8,(26.7%)	3.40	1.192
Scale:1(Strongly Agree) = SA, 2(Agree) = A, 3(Disagree) = D, 4(Strongly,Disagree) = SD, 5(Dont Know) =DN. N=20 (faculty), WA= Weighted Average.,S.Dev. = Standard Deviation.							

On the basis of reply on whether or not MIST has a formal IT security awareness program for faculty, analysis showed that (One hundred) 100% faculty member did agree on this.

4.2.4 Evaluation of present IT management system

4.2.4.1 IT Security success evaluation

On a scale of 1 to 5, evaluative question feedback from the faculty showed in Table 4.3 (*see* Table A.6 Appendix-A).Only (ten) 10%agreed that MIST is equipped with successful IT management system, while (forty-five) 45%disagreed and (twenty-five) 25%strongly disagreed with the statement. Rest of the respondents answered indefinitely.

Table 4.3: IT Security success evaluation

My,Institute is equipped with successful IT security management system?(faculty)	Response on IT Security Success Evaluation Patten (N=20),(Frequency (Percentage of Respondents))						
	SA	A	DA	SD	DN	WA	S.Dev
		2,(10%)	9,(45%)	5,(25%)	4,(20%)	3.55	0.945
Scale:1(Strongly Agree) = SA, 2(Agree) = A, 3(Disagree) = D, 4(Strongly,Disagree) = SD, 5(Dont Know) =DN. N=20 (faculty), WA= Weighted Average.,S.Dev. = Standard Deviation.							

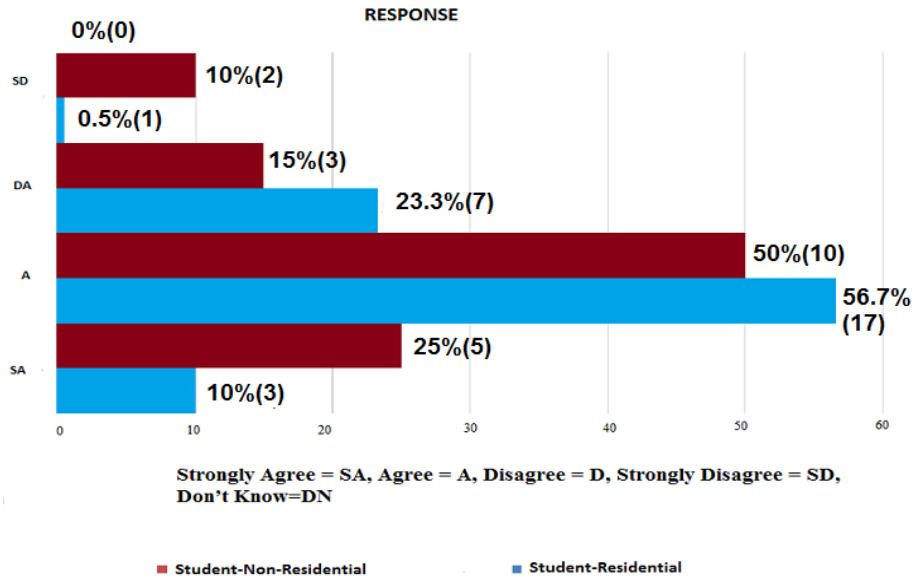

Figure 4.2: Response on IT Security as a Top Confronting Issue (N=50)

4.2.4.2 IT Security as a Top Confronting Issue

According to both residential and non-residential students of MIST, this study has found IT security is one of the three top IT issues confronting the institution today. The bar chart (*see* Figure 4.2 , Source:Appendix A.2 & A.3) showed that more than (fifty) 50%from each of the residential and non-residential students agreed with the above statement.

The bar chart (*see* Figure 4.2 , Source: Appendix A.3) showed that more than (fifty) 50%from each of the residential and non-residential students agreed with the statement that IT security is in the top three concern of MIST authority.

4.3 Analysis

4.3.1 Critical Analysis

IT security strategy of MIST covers both short and midterm vision at present focusing a long term security to be undertaken in near future. The infrastructure of IT security is underway and taking a holistic effort in day to come. MIST has well organized IT cell headed by OIC, IT cell, IT personnel dedicated for specific responsibility. IT cell runs with dedicated professional experts (more than five) who are qualified in IT and given responsibilities that are spread across multiple functions. MIST has formal and well-practiced IT security policy monitored and updated regularly which was in vogue since last at least five years or more. The policy adopted covers appropriate use of institutional IT assets, enforcement of institutional security policies, desktop security(anti-viruses etc.), system access control(password management, authorization, authentication, data access, privilege management, physical security of IT assets, network security(firewalls etc.), resident halls, remote devices and authority to shut-off internet access. Qualitative approach summed up that MIST has a comprehensive, regularly updated, consistent and easy to read IT security policy where respected Dean of MIST, Head of the department of Computer Science and Engineering (CSE) and OIC IT cell were actively involved to input their thoughts, while quantitative research approach supported the fact with the limitation that yet a great many concerned IT users need to be made aware of such policy.

Certainly the analysis brought out that IT security forms an integral part of strategic plans of MIST which is at present undergoing strict scrutiny, validation and approval to be implemented as soon as possible. However quantitative part identified the lack of digital repository dedicated to faculty members for storing confidential and secret data. MIST aware faculties and staffs about IT security and how best they can act securely in modern days IT threat and vulnerabilities, on which the staff, faculty and IT personnel agreed to be effective for all concerned. However a mixed to negative feed were found from students. Some

students were found ignorant about existence of such type of program. As per qualitative assessment there are daily monitoring of networks, operating systems for vulnerabilities and attempts at unauthorized access. Limiting the types of protocols allowed through firewall/router, limiting the URLs allowed through firewall/router and restricting and eliminating access to servers and application are already implemented to reduce IT security vulnerability. Timing out access to specific application, using security devices(cards, biometric scanners etc.) for personal authentication and Instituting a recovery or back up plan in the case of disasters caused by natural events or by human acts are the enterprise processes under consideration to implement for reducing IT security threat and vulnerabilities. IT security incidents were reported to higher officials/personnel concerned on as and when basis. Though present budget on IT security was least mentionable but IT cell OIC expected an increase in staffing, hardware/software/products and education/training in upcoming year.

Evaluation on the IT security programs for MIST got a fairly successful feedback after qualitative analysis and judged as more secured IT environment than it was at least four years back. Interestingly the faculty gave a mixed feedback while maximum of students agreed on the issue. Hence the status of IT security program remained on average side and needed improvement.

4.3.2 SWOT Analysis of MIST towards Implementation of a Robust IT Security Management Framework

A SWOT analysis (alternatively SWOT matrix) is a structured planning method used to evaluate the strengths, weaknesses, opportunities and threats involved in a project or in a business venture.Users of SWOT analysis need to ask and answer questions that generate meaningful information for each category (strengths, weaknesses, opportunities, and threats) to make the analysis useful and find their competitive advantage. SWOT analysis can be used effectively to build organization or personal strategy. Steps necessary to execute strategy-oriented analysis involve: identification of internal and external factors, selection and evaluation of the most important factors and identification of relations existing between internal and external features. Hence, SWOT analysis of MIST towards implementation of a Robust IT Security Management Framework should bring effective outcome.

The SWOT analysis is necessary to provide direction to the next stages of the change process. In our case study to Identify barriers that will limit goals/objectives SWOT analysis should fit perfectly and thereby, help MIST to systematically step forward with critical strategic measures. The outcome that were identified are categorized under four heads in SWOT matrix(*see* Table 4.4).Strengths and opportunities are the internal factors of MIST, while threats and opportunities are external factors dictates the next step from policy makers point of view. The analysis being a scientific analysis tool is very effective and aligned

the process of our case study. MIST should asses following the example shown so that the result is as effective as the system itself. IT security possessing the dynamic nature of progress must therefore be assessed logically and systematically coping up with the strategic and operational strength of the case Institution. Therefore, a reasonable approach taking into consideration that the threats and weaknesses i.e. the external factors might hinder the objective should be devised through SWOT. There lied the purpose of the intended study.

4.4 Discussion

MIST has a concrete, meaningful long-term vision about Higher Education and thus IT involves related IT personnel in developing and adopting the strategy and operational plan. IT OIC heads the IT cell of MIST which is run with dedicated professional experts (more than five). All IT personnel are qualified in IT and given responsibilities that are spread across multiple functions. The policy adopted covers appropriate use of institutional IT assets, enforcement of institutional security policies, desktop security(anti-viruses etc.), system access control(password management, authorization, authentication, data access, privilege management, physical security of IT assets, network security(firewalls etc.), resident halls, remote devices and authority to shut-off internet access. The IT security policy is easy to read and concise in nature.

IT practice in MIST have lacking in storage option for the faculty members to store individually managed confidential data in digital repository. MIST uses authorization through password and MAC address. IT security awareness program was not fruitful with the students though the faculty and IT staffs gave positive feedback about the program. MIST runs successful model of Enterprise Processes by limiting the types of protocols allowed through firewall/router, limiting the URLs allowed through firewall/router and restricting and eliminating access to servers and application to reduce IT security threats. Furthermore, Timing out access to specific application, using security devices (cards, biometric scanners etc.) for personal authentication and Instituting a recovery or back up plan in the case of disasters caused by natural events or by human acts are planned for future implementation.

Though the IT officials claimed their success to improve the IT management system but mixed feedback from the faculty made the status of IT security program to put on average side and made the candidate for further improvement. Since security is an ongoing process and gradual updating is the basic requirement, so the discussion lead to an IT management system that definitely has much scope to improvement. A study therefore summed up with clearer insight of strategy, policy and practice of IT security management system of MIST.

4.5 Summary

MIST has formal IT organization to ensure IT security in the parameter laid down through a concise and effective strategy and policy. Its awareness program needs to incorporate the students of all levels and follow an integrated approach. However an Enterprise process is evaluated against MIST and feedback of related personnel gave a fairly good feedback. Hence we can consider that a workable set up is running in the context of enterprise process for IT security management system. Though the IT officials evaluated their management system as successful but mixed feedback from the faculty made the IT security program a definite candidate for further improvement. At present the authority of MIST are undertaking a series of development measures in IT security management system field. Few of those steps are already in action while most are in the process of implementation.

Table 4.4: SWOT analysis on MIST,(IT Security Management System)

SWOT analysis on MIST,(IT Security Management System)	
Strengths	**Weaknesses**
Extensive,and diversified IT portfolio	Significant,focus on Competitive Outputs only.
Advertising and marketing capabilities	Undiversified,User portfolio
Strong,partnerships with internal and external stakeholders.	Certain,level of Budgetary Constraints due to bureaucratic dilemma
Leading,player in the global beverages industry	Negative,or Rigid mindset to adopt any change
Brand,recognition and reputation in the Higher Education arena	Risk,avoidance, insignificant innovation strategy and less initiative to IT,security management system incorporation
Organized,and Robust Organizational Chain of Command.	Bottleneck in regards to Sponsored Research and Financial back-ups or Handling parallel Curricula besides Extra Curricular Research Initiatives
Extensive,IT security Management and distribution channels	
C4,(Command, Control, Communication and Computer) along with inherent,Centralized Authority by MoD (Ministry of Defense).	
Robust Strategic, goal-oriented and Operational Policy.	
Well,laid IT infrastructure	
Opportunities	**Threats**
IT,sectorial growth in MIST	Dynamism,in user choice, awareness program, accordingly fulfil the demand
Increasing,demand for enhanced IT security management system	Lack,of flexibility in policy change
Growing,IT user and consumption in emerging IT system of MIST (Faculty, administration, Student, IT personnel etc.)	Difficulties,in striking a balance between Top priorities in IT Management
Growth through behavior, day-to-day techno convergence, impact of national and international IT invention and availability.	Visible and measurable return on IT security management system may not always convince the concerned policy makers.(Thus making the system reactive to some extent)

CHAPTER 5
CONCLUSION AND RECOMMENDATION

This study focused on assessment of IT security management system in MIST by evaluating the strategy, policy and practice with an to achieve a clearer conceptual understanding of present IT security state of readiness, behavioral aspects in relation to establish IT security and bring out measurable outcome to reshape a more enhanced IT management system in MIST. Thereby this study believed to input significant contribution on the information security efforts of MIST. Given that only one representative of Higher Education IT management system was selected i.e. MIST, this result might not produce much generalization for all other Educational Institute of Bangladesh but could be counted as an in-depth and benchmark effort.

5.1 Conclusion

Most of the cases this study found a positive framework of strategy, policy and practice that governing the perceived IT security management system of MIST. Contrary to the findings of literatures, this study found, crisis had not produced an immediate negative impact. Though few of the fields were yet to outreach the intended target group within the awareness and risk assessment parameter. This research also partially supports, proactive measurement enable MIST to cope with the crisis influence on combating IT security threats and vulnerabilities. The analysis noted, One of the leading high quality Higher Educational Institute like MIST are less likely to misconduct, mislead and fall apart when sudden strategy, policies and practices are well rehearsed and validated in temporal and spatial perspective in countering IT security threat and vulnerabilities.

This study assessed the IT management system from qualitative and quantitative point of view to asses and evaluate the established and believed culture in IT security that is considered in MIST to be an ongoing Improvement process. It helped to self-assess and to create a sense of alertness in speeding up the process against worldwide incidents of IT breeches to act more proactively. Further study scope on the same field was left wide open and have great potential to be explored in multidimensional perspective. The research would be considered helpful to input their outcomes and to benefit other Higher Education Institute, Non-profit Organization, Government and Non-Government Organization.

It is way farfetched to assume a direct link between established IT security culture and the satisfactory IT security guaranteed. This research simply sought to demonstrate IT management system and logically reasoned human behavioral aspect that has direct or indirect impact on ensuring suggested secured IT management system within the outfit. Findings suggests that MIST has a satisfactory and workable strategic goal with operational planning of adopting modern day updates, technological behavior, well laid down policy of who does what and a long term vision of IT security bench mark to achieve. An easy to use mobile application was devised with the outcome of the case study that will help aware users of IT assets and improve their secured behavior benefiting MIST. Definitely the suggested improvement texture on the aspect of executable Soft Intervention in balanced approach will help mitigate IT threat and vulnerability. Also, it will benefit and facilitate the organization with an improved IT Security management and execution framework. The problem specification of this paper will act as the center point of the researchers innovation and analysis of different existing techniques will assist them being a knowledge hoard in their progress of further research work.

5.2 Recommendation

After having drawn the conclusion and summary of all the major study points, some recommendation are made in this section which the researcher believe could enable MIST and Organizations with similar diversified nature dealing with IT security to improve in their organizational execution framework:

- Re-assess the present IT strategies and initiate a comprehensive appraisal technique incorporating both tangible and intangible motivation based on the expected level of IT security. And this appraisal process must need to be dynamic and should be revised periodically to logistically determine the employee and new users needs, behavior pattern, culture, value and expectations in accordance with the Organizational vision and objective.

- The need for easily accessible, well transmitted, clear,concise and comprehensive IT security policy across the Institute to be devised and incorporated with the existing policy can never be underestimated.

- The next one is to develop a framework of how to combat multifaceted IT security threat within the context of world-wide IT security breech e.g. IT security incidents in universities, hacking, penetration, intrusion etc. are real threats. And while framing its shape this study recommends having a long term policy on the followings:

Assessment of IT practice as how successful it was on a regular basis, awareness program, motivation of IT users and stakeholders and flexibility of incorporation of rapid change of IT security measures.

- Along with the organizational risk assessment system for the IT practice all the internal departments are suggested to have their own of it in their arena and exercise it preciously to further strengthen the prospective and existing IT security culture to act holistically.

- Organization need to emphasize on the personal development plan through training, recruitment of IT consultant and professionals, run certification courses, accepting only qualified IT experts etc. for all of its employees. Thereby to assist them to have a balance between their desires expectation and organizational provision which ultimately could lead towards more secured IT management system.

- MIST may plan Single sign-on through Kerberos. MIT for example continues to implement its security strategy using Kerberos, X.509 certificates and strong machine- and application-based defences.

- Foster a bottom-up approach to security. MIT recommends that participation be as broad as possible for security. Communicate problems but not to confront as because of the participative nature of IT security policy adaptation and execution requirement in MIST.

- Timing out access to specific application, using security devices(cards, biometric scanners etc.) for personal authentication and Instituting a recovery or back up plan in the case of disasters caused by natural events or by human acts are the enterprise processes might be chosen to implement for reducing IT security threat and vulnerabilities.

- IT security approaches which might benefit MIST at large scale are (a) Centralized data backup system (b) Secure Socket Layer (SSL) (c) Intrusion detection (d) Intrusion prevention tools (e) active content monitoring/filtering.

- Awareness program can be more excelled where in an easy to use mobile application that were devised as sample for the part of this case study should be found helpful.

- Digital dedicated repository for faculty would enrich and motivate more quality research in upcoming days for MIST.

- Time lag between deployment of technology and the development of legal and policy framework for appropriate use, resources and awareness barriers must be improved or removed as they were found by the IT users as IT security impediments in MIST.

5.3 Future Study

MISTs experience demonstrates the essential roles that both technology and people play in maintaining a successful IT security program. MISTs technical innovation has resulted in a robust solution that preserves openness in an increasingly unsafe network Management System, but its IT security student, staff, employees and faculties have proven just as important to its success. This latter point is particularly important because many Institutions may not have the resources to emulate MISTs security architecture and culture, but they can foster a similar cultural management system to enhance IT security institution-wide in Bangladesh.

The problem specification of this paper will act as the center point of the researchers innovation and analysis of different existing IT security measures in Higher Study Institute and any other similar natured organization will assist them being a knowledge hoard in their progress of research work.

In future beside the technological fortification, the human perspective of IT security should be found more interesting and challenging field to study. Definite scope of modern day trend analysis in strategic and operational balance between the organizations IT security vision is going to get emerged. Psychological trend of IT criminals, socioeconomic cultural effect on IT security effort, users behaviour and value added with their expectation from IT and participation of individuals holistic approaches of IT security are going to get more attention in upcoming IT security assessment study.

REFERENCE

[1] C. Colwill, "Human factors in information security: The insider threat–who can you trust these days?," *Information security technical report*, vol. 14, no. 4, pp. 186–196, 2009.

[2] N. S.Talib and S.M.Furnell, "Establishing a personalized information security culture," *International Journal of Mobile Computing and Multimedia Communications (IJMCMC)*, vol. 3, pp. 63–79, 2009.

[3] R. YANOSKY, "Identity management in higher education: A baseline study," *EDUCAUSE Center for Applied Research*, vol. 2, 2006. Last accessed on December 06, 2014, at 10:08:00PM. [Online]. Available: http://www.educause.edu/ecar/.

[4] A. Dodge, "Educational security incidents (esi) year in review–2009," 2009. Last accessed on July 29, 2014, at 08:08:00PM. [Online]. Available: http://www.adamdodge.com/esi/yir2009/.

[5] R. B. Kvavik and J. Voloudakis, *Information technology security: Governance, strategy, and practice in higher education*. Educause, 2003.

[6] R. A. Popa, C. Redfield, N. Zeldovich, and H. Balakrishnan, "Cryptdb: protecting confidentiality with encrypted query processing," in *Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles*, pp. 85–100, ACM, 2011.

[7] M. Dark, R. Epstein, L. Morales, T. Countermine, Q. Yuan, M. Ali, M. Rose, and N. Harter, "A framework for information security ethics education," in *10th Colloquium for Information Systems Security Education-University of Maryland*, vol. 4, pp. 109–115, 2006.

[8] D. Ward and B. L. Hawkins, "Presidential leadership for information technology.," *Presidency*, vol. 6, no. 2, pp. 1–11, 2003.

[9] M. J.Arafat, G.M.Daiyan, "Emergence of robust information security management structure around the world wid structure around the world wide higher education e higher education institutions: Institutions: a multifaceted security solution multifaceted security solution multifaceted security solution," *IJCSI*, vol. 9, 2012.

[10] A. Fal, "Standardization in information security management," *Cybernetics and Systems Analysis*, vol. 46, pp. 512–515, 2010.

[11] Y. Cherdantseva and J. Hilton, "A reference model of information assurance & security," in *Availability, Reliability and Security (ARES), 2013 Eighth International Conference on*, pp. 546–555, IEEE, 2013.

[12] A. C. Yeo, M. M. Rahim, and L. Miri, "Understanding factors affecting success of information security risk assessment: The case of an australian higher educational institution," 2007.

[13] J. H. Dexter, "The cyber security management system: A conceptual mapping," *Global Information Assurance Certification*.

[14] D. J. Staley and D. A. Trinkle, "The changing landscape of higher education," *Educause Review*, vol. 46, no. 1, pp. 16–33, 2011.

[15] E. Dahlstrom, J. Walker, and C. Dzuiban, "Ecar study of undergraduate students and information technology, 2013. louisville: Educause," 2013.

[16] Last accessed on December 10, 2014, at 10:00:00AM. [Online]. Available: http://hack-lol.blogspot.com/2012/03/military-institute-of-science-and.html/.

[17] Last accessed on December 08, 2014, at 11:00:00AM. [Online]. Available: http://www.ehackingnews.com/2012/06/cyber-war-more-bangladesh-government.html/.

[18] J. Pirani, "Sheep pond associates & ecar.(2003).incident response: Lesson learned from georgia tech, the university of montana & university of texan at austin," *Case Study, ECAR*, no. 7.

[19] B. Taylor, S. Kermode, and K. Roberts, "Research in nursing and health care: Creating evidence for practice," 2006.

[20] D. M. Mertens, "Transformative paradigm mixed methods and social justice," *Journal of mixed methods research*, vol. 1, no. 3, pp. 212–225, 2007.

[21] R. Singh, M. Keil, and V. Kasi, "Identifying and overcoming the challenges of implementing a project management office," *European journal of information systems*, vol. 18, no. 5, pp. 409–427, 2009.

[22] U. Sekaran and R. Bougie, "Research methods for business: A skill building approach. wiley," 2010.

[23] P. Dahler-Larsen, *The evaluation society*. Stanford University Press, 2011.

[24] D. M. Fetterman, *Ethnography: Step-by-step*, vol. 17. Sage, 2010.

APPENDIX A
SPSS ANALYSIS

A.1 SPSS Figures

Does your organization provide you with confidential digital repository for your classified materials (administrative and academic)? (Faculty) (N=20) *see* A.1

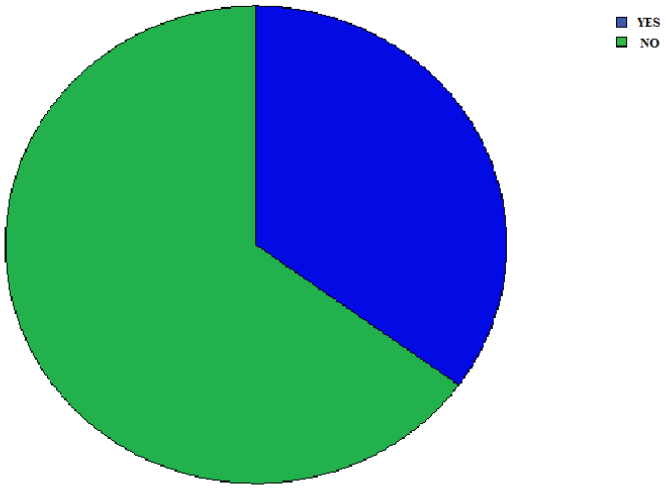

Figure A.1: SPSS data for Figure 4.1

IT security is one of the three top IT issues confronting my institution today. (Student-Residential and Non-Residential) *see* (N=50) A.2 & A.3

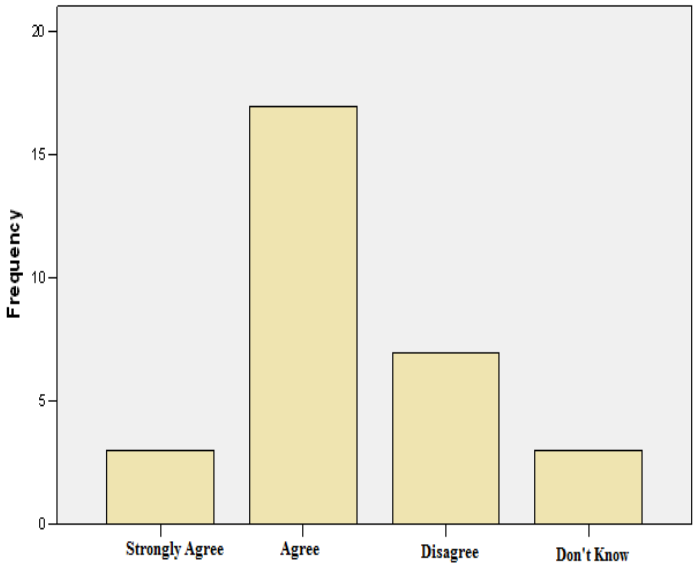

Figure A.2: SPSS data for Figure 4.2

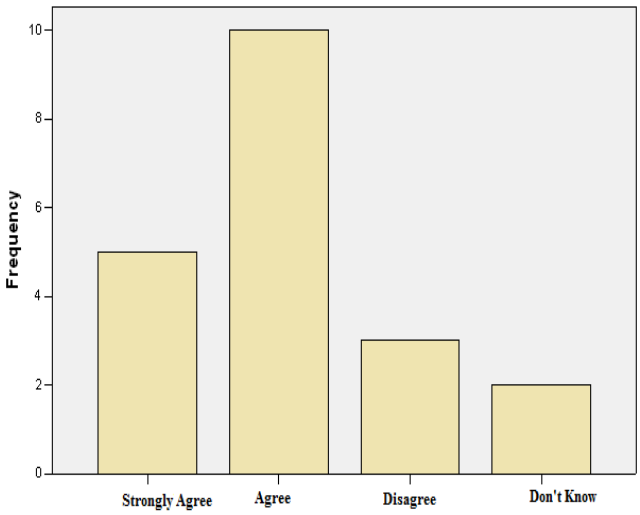

Figure A.3: SPSS data for Table 4.2

A.2 SPSS Tables

My institutions has IT security policies that are clear and easy to read(faculty) *see* A.4

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	9	45.0	45.0	45.0
	Disagree	5	25.0	25.0	70.0
	Strongly Disagree	2	10.0	10.0	80.0
	Don't Know	4	20.0	20.0	100.0
	Total	20	100.0	100.0	

Figure A.4: SPSS data for Table 4.1

My institution communicates IT security awareness issues for its students(Student-Non-Residential) *see* A.5

My institution communicates IT security awareness issues for its students(Student-Residential) *see* A.6

My Institute is equipped with successful IT security environment?(faculty) *see* A.7

		Frequeny	Percent	Valid Percent	Cumulative Percent
Valid	Strongly Agree	2	10.0	10.0	10.0
	Agree	6	30.0	30.0	40.0
	Disagree	6	30.0	30.0	70.0
	Strongly Disagree	3	15.0	15.0	85.0
	Don't Know	3	15.0	15.0	100.0
	Total	20	100.0	100.0	

Figure A.5: SPSS data for Table 4.2

		Frequenc y	Percent	Valid Percent	Cumulative Percent
Valid	Agree	9	30.0	30.0	30.0
	Disagree	8	26.7	26.7	56.7
	Strongly Disagree	5	16.7	16.7	73.3
	Don't Know	8	26.7	26.7	100.0
	Total	30	100.0	100.0	

Figure A.6: SPSS data for Table 4.2

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Agree	2	10.0	10.0	10.0
	Disagree	9	45.0	45.0	55.0
	Strongly Disagree	5	25.0	25.0	80.0
	Don't Know	4	20.0	20.0	100.0
	Total	20	100.0	100.0	

Figure A.7: SPSS data for Table 4.3