Emergence of Robust Information Security Management Structure around the world wide Higher Education Institutions: a Multifaceted Security Solution

Jahidul Arafat[1], Golam Moktader Daiyan[2] and Md. Waliullah[3]

**[1] Department of Computer Science and Engineering, University of Liberal Arts Bangladesh
Dhaka, Bangladesh**

**[2] Department of Computer Science and Information Technology, Southern University Bangladesh
Chittagong, Bangladesh**

**[3] School of Computing & Mathematical Sciences, University of Greenwich
London, UK**

Abstract

Polarizing the views on the emergence of Information security around the campus arenas of higher education institutions is the utmost erg of both developing and developed nations in this post catastrophic era of September 11, 2001 where 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, however 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 of these regions. Addressing this issue, a new security management scheme namely Robust IT Security Balancing (RITS-B) Approach is proposed in this paper 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. A quantitative survey has been conducted and the security facts and findings are compared with the three basic survey questionnaires namely more secure than two years ago, system is secure and security program is successful with a 4 point likert scale. The analyzed data shows that institutions which implemented RITS-B approach in their arena either partially or fully feel more high in the above three domains than the others and thus increases the application area of the soft security solutions.

Keywords: ***Information Security, Governance, Strategies, Practices, Regional Cultures and Believes.***

1. Introduction

Information technology security in higher education is the process of securing the higher education environment without disrupting the openness, accessibility, academic and intellectual freedom which is at the very heart of the higher education environment. It is one of the fundamental process towards the broader security because the further processing steps depends of what types of security breaches has been occurred and what strategies are in place to cope up with these. Despite the numerous functionality of security, IT security in Higher education is still a subject of on-going investment and it cannot be conclusively stated that education field is highly secured because of the application, technological and intrusion's diversity. As a consequence, the task of choosing the best method which will not only ensure mission critical level security to each bit of higher education information but also not compromise with its core missions is still a difficult challenge. Several survey papers (Arabasz & Pirani, 2002; Kvavik & Voloudakis, 2003; Yanosky & Salaway, 2006) cover 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

Basically, the first approach explores the information security technologies used by the higher education institutions. What tools have they chosen to install, to prevent harm to their information assets? The security levels are then deduced from the boundary of these installed high functional tools. The usual tools that are

Copyright (c) 2012 International Journal of Computer Science Issues. All Rights Reserved.

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 and shibboleth. The first approach fails to gain total effectiveness in the higher education information security process due to the following reasons: (a) Money matters when developing IT security strategies but much depends on how, when and where it is used, by whom and with what level of effort and skill. (b) Integrating adopted technologies with current and future practices is the lion's share then just that of selecting it. (c) And peoples' troubles in understanding the adopted technologies (Yanosky & Salaway, 2006).

The strategies for the second approach exploit the importance of soft IT interventions (e.g. organization, Cultural aspects, awareness program, training programs, policies, executive attention etc.) to produce a secured campus environment around the educational institution and having the 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 environment 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 called Robust IT Security Balancing (RITS-B) Approach is presented in this paper. This is an attempt to unify different methods of higher education information security approaches under a common topology based on the both hard and soft interventions with that of Muslim culture and believes. This RITS-B Approach considers all the soft aspects of information security i.e. information security Policies, Awareness, Leadership and Practices for the user community on the acceptable use of technological tools to develop such strategic framework of security environment where facts, national and religion 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. In the RITS-B approach, soft security aspects are used not to describe which contents should they have rather what should be the status of these in place security aspects and what characteristics should they bare for the acceptable use of the existing security tools and technologies to the campus community and thereby to secure their information arena.

A quantitative survey on 6 engineering universities of Bangladesh shows that institutions which implements the proposed RITS-B approach either fully or partially in their arena characterized their security program's success much more higher than others and also reported that their data, networks and applications are more secure and feel more secure today than it was two years before.

This paper is organized as follows: the literature review related to the basic idea on higher education IT security around the Muslim nations and various hard and soft aspects of security to secure their arena including their advantages and disadvantages is detailed in section II. The RITS-B approach is presented in section III. The quantitative survey results are provided in section IV and finally section V shows some concluding remarks.

2. Literature Review

Though there are huge numbers of Information security balancing approaches in the literature (Executive Guide, 1998; Fender, 2006; Gray, 2005; Rivlin, 1995) the Soft IT Security (SITS) approaches on the acceptable use of security hard interventions are only considered in this paper. For this reason, the related literature based on the SITS approaches is presented as follows.

2.1 Basic Idea on Higher Education Information Technology Security

By far the most commonly used meaning for information security is the preservation of (Dark et al, 2006; Voloudakis & King, 2003; Ward & Hawkins, 2003):

(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 and

We can, in turn, characterize each of these seven protection categories: confidentiality, integrity, authenticity, scalability, non-repudiation, accountability,

Copyright (c) 2012 International Journal of Computer Science Issues. All Rights Reserved.

and availability-by levels of sensitivity: high (serious injury to an institution), medium (serious injury), and low (minor injury). These hints are significant for higher education, where much information used for teaching and research requires the highest level of integrity and availability but low level of confidentiality and for Muslim nation flexible sense of scalability also need to be defined. And to ensure such level an institution have two choices: either to follow the security approach (a) or (b) as mentioned in section I or go for the use of a blended approach- balancing the features of (a) and (b) according to its academia's believes, needs and constrains to foster the institution's security goal. Where this balancing scheme requires the exploration of the following issues (Bellovin et al, 2006; Albrecht & Caruso, 2003; Pirani, Sheep Pond Associates, Voloudakis, Ernst & Young, 2003):

1. Make IT security a priority.
2. Selecting security controls and products.
3. Defining and empowering acceptable behavior [by students, faculty, and staff].
4. Preserve the academia's religion, regional and cultural believes.
5. Revise instructional security policy and improve the use of existing security tools.
6. Making consistent, timely, and cost-effective management decisions.
7. Improve security for further research and education networks.
8. Integrate work in higher education with national effort to strengthen critical infrastructure and
9. Empowering [members of the institution's community to do their work] securely.

And all these are the pledge of the higher education to gain success in openness and privacy in the field of information security.

2.2 Security Management by Hard/Soft Interventions

Balancing IT security approaches by 'Hard' interventions is a procedure that groups the technological requirements and academia's culture and needs into a broader area. The simplest approach is the security technology aggregation, which starts with a set of "Hardware/ tools" requirement around the campus boundary. From these, security collaboration grows by appending the functionality of each tool 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. But, it is suffering from the following six immediate problems (Ellen & Luker, 2000; Kvavik & Voloudakis, 2003; Visa Inc., 2004; Sieberg, 2005):

- Academia's resource and budgetary constrains
- IT security does not appear to be high on most Islamic institutions' executive agenda
- The "transient" nature of the higher education's constituents complicates the IT security management
- The rapid changing nature of the intrusions.
- Resource may become burden and garbage if they are hard to use and understand.
- And as because of the security solution which seems to be convenient for a particular educational environment at time 't' may become inconvenient at time't+1' because of the transient nature of threats and academic requirements.

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 (Yanosky & Salaway, 2006; Rezmierski, Rothschild, Kazanis & Rivas, 2005).

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 academia's values i.e., freedom and openness and academia's 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 academia's 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 Big Boss rather the twin brothers 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

Copyright (c) 2012 International Journal of Computer Science Issues. All Rights Reserved.

appropriate use can also hinder the security outcomes (Pirani, Sheep Pond Associates & ECAR, 2003).

3. Proposed Model

To enhance the performance of the security balancing process and to address the drawbacks of only having the hard i.e. technological aspects of security solution as mentioned in Section II 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 to flourish the fragrance of technological aspects over their acceptable use around the campuses of worldwide Muslim nations.

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 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) Academia's values and believes which has produced the requirements of these fives and other consequent security requirements generated by these ethical concerns.

In this RITS-B approach information security balancing process is summarized into four (04) stages: Identification-Prioritization-Revision-Dynamicity which is briefed as follows to fulfill the requirements of (1) to (9) of section II. (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.

Since definition of the security scope and strategies is the first stage of the proposed RITS-B approach, it is detailed in the next section.

3.1 Definition

For an institution to make its security environment more reliable and sophisticated to breach, its scope of application along with the strategic scale for assessment must need to be defined. The following subsections depict such definitions.

3.2 Define the institution's information security scope

In a bigger sense scope is something that helps an institution to find out its field and purpose of application and flexibility to sustain. For an institution this scope definition involves two preliminary phases that must need to be done before heading further and these are:

- Develop a framework of security environment where facts and national perspectives will be merged up to lead to a proactive leadership and cyber security system without violating the freedom and openness that is at the very heart of our academic values.
- Identify what security policies, tools, and procedures are currently in place and which pattern needs to be practiced to ensure a high degree of cyber security around the campuses of higher education institutions of Muslim nations.

3.3 Define the IT Security Strategic Assessment Scale

Based on the use of the technological and cultural aspects the following four major strategies scales or approaches (Figure 1) can be used to find out the institution's existing security status and thereby securing them on the basis of their strength in each arena. And these are: (i) Reactive (ii) Cultural (iii) Technology Centric and (iv) Fortified.
Reactive approaches tend to have investment relatively little in either (a) or (b-e) while cultural approaches have higher investment on (b-e) but relatively little in (a). The technology-centric approach is just opposite to the cultural one having high on (a) but very little in (b-e), where relatively higher investment in both (a) and (b-e) is the scheme of the fortified approaches. Most of the IT security approaches use about all of these six requirements. Value criterion is used to find out the academia's believes and needs and (a-f) are blended in a proportionate fashion based on the academia's requirement to secure its environment and this blending scheme should not be a conclusive one and also should not be the one way traffic to become responsive to the changing environmental nature rather it should fall in the above circular shaded area.

After defining the scopes and scale of intended institution's security concern, a documentation of its hard

Copyright (c) 2012 International Journal of Computer Science Issues. All Rights Reserved.

interventions is needed to formulate an acceptable soft layout on them to gain robustness in the process of information security and secrecy. And this documentation stage is presented in the next section.

3.4 Document the institution's technological needs

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 use different set of tools. The ultimate goal is to fulfill the requirements of (1) to (9) of section II.

The next step is to formulate an exact soft security layout on the documented security hard interventions with that of the scope. The following section depicts this step of formulation.

3.5 Formulation of Acceptable Soft Security Layout

The soft stage of 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.

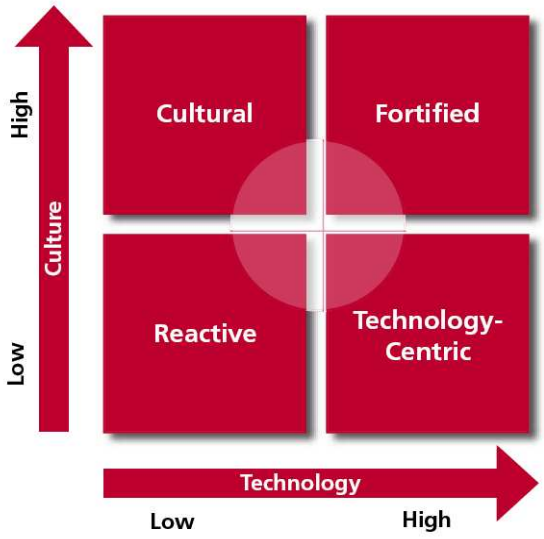

Fig 1: IT Security Approach

3.5.1 Model Management System Information Security on campus

The model management system campus information security is based on the context of Define-Implement-Analyze-Improvement i.e. **DI-AI** methodology as presented in the following figure.

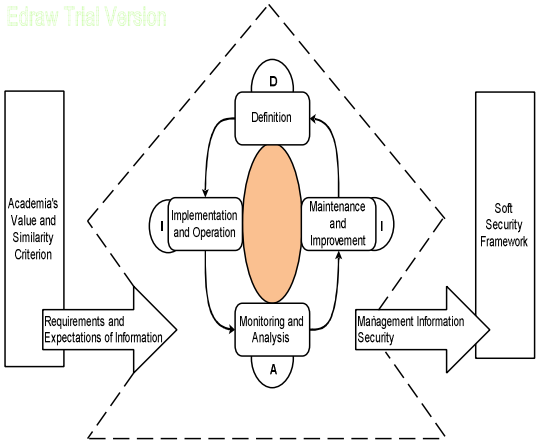

Fig 2: DI-AI Methodology

Define the scope, objective and significance of the existing security concerns along with that of institution's value and similarity criterions as described above and make a plan to implement. Then go for its implementation while at the same time monitor and analyze the implementation process and outcomes respectively. Do possible maintenance and if necessary take necessary improvement actions to gain inclusiveness in the process of campus information security.

Copyright (c) 2012 International Journal of Computer Science Issues. All Rights Reserved.

For the institution's to proceed on the above mentioned DI-AI methodology in this security balancing process, they should follow the standards of NBR ISO/IEC-27001:2005, "Management System Information Security". In the light of this standard, institutions should designate an individual to be responsible for IT security and these key responsible personnel should report to their respective senior management in a periodic fashion and should bare a certain level of security certification. Even though certification don't prove knowledge but shows that concerned personnel has putted their time and effort to gain the specialized skill. The institutions also need to have a well defined salary structure for these IT security personnel.

Institutions are also recommended to apply this methodology on the resources of infrastructure services provided by their respective Data Centers to ensure the assistance of the Information Security Policy and its objectives in this robust security balancing process, which were defined by the High Authority.

3.5.2 Model Information Security Organizational Structure

The next step towards the implementation of the above mentioned management system is to shape a well defined security organizational structure. Absence of a robust security organizational structure may hinder the security implementation. The modeling of this security organizational structure should follow the following scripts:

1. Establish a central security office.
2. Decentralize the functionalities of this office into two wings: the Information Technology Policy Office (ITPO) and the Information Technology Security Office (ITSO).
3. The ITPO will handles IT policy development, dissemination, and education, and the ITSO will handles security analysis, development, education, and guidance for respective institution's information assets and IT environment.
4. Moreover, institutions should have at least some dedicated security staffs to fulfill the functionalities of the above two wings.

3.5.3 Development of security plans and policies

To implement the above mentioned management and organizational system, it is essential to have a well defined security policy and plan with the rules on servitude and degree of practicum across the institutions.

It is important to note that a significant drawback of SITS approach is that it may inhibit the academic freedom by limiting access to certain necessary information for which people may not comply with the security process towards its implementation. Moreover people may find it difficult to understand the derived policies. Absence of a periodic review pattern on the existing policies can make the further damage. So the development of a robust security policy and process should follow the following scripting as enlisted below:

1. Consider the value criteria of a particular educational institution while driving policies where policies dictate processes, procedures, and standards; and security implements those.
2. Policy should be accessible - clear and easy to read - consistent across the institution – enforced - regularly updated - and comprehensive.
3. All the campus community's users are instructed to understand their participation in the care that the information security policy.
4. Involve Senior Management in information security Policy and Plan development phase. And a discussion need be done among representatives from all sectors of the institution and should be done periodically.
5. Evaluate the just-in-time suitability of the existing security policies during the critical analysis of the Management System Information Security and where appropriate, be revised and if possible re-train all the security employees and make the user community aware about it.
6. Finally, provide a framework to merge all of the above to gain robust scalability, sustainability and secrecy in this policy derivation-codification-modification and application process.

And for ensuring the policy's implementation, institution must need to have either a partial or comprehensive plan in place. One thing to keep in mind that, institution's IT security policy and plan should not only supports academic freedom but also ensure ready and timely access to information to authorized users and its smooth execution while preserving the academy's most important values into the arena that some might otherwise find problematic. A good security policy and plan can play an important role in liability abatement by demonstrating that the institution has taken appropriate and necessary precautions to protect its information assets.

3.5.4 Communication and awareness

A policy cannot be effective by itself. Neither it nor the IT security organizational structure produces a subjectively

Copyright (c) 2012 International Journal of Computer Science Issues. All Rights Reserved.

appropriate security until there are some awareness programs regarding these. The following twos depict how the awareness activities should looks like.

1. Institutions must conduct awareness activities for users to ensure they understand and trust the policy and for staff members who configure and use security technologies in a periodic fashion.
2. To further build confidence continuous security education is likely to be one of the most cost-effective and important defensive strategies for an institution to take.

The lack of attention to security is a long-standing situation and has led to a huge awareness gap. A biggest concern is that very large portions of the people who connect to the network have no concept of security and [are] showing up with improper setups. That's why institutions should invest in a very high degree of awareness. Awareness building does not have to cost a lot of money, but it definitely needs attention.

3.5.5 Model the pattern of institutional IT Security Practices

The next step towards the implementation of the RITS-B approach is the definition of IT security practices i.e. Methodology for Analysis and Evaluation of Risk of Information Security, for Updating and Maintaining Systems and for access Control Procedure and Detection-Monitoring Process. Since we are dealing with security, or in any branch of human activity, it is natural to know the risks involved. This will be done through a deep analysis.

The Risk Assessment and Audit (RAA) is performed by a Work Team with representatives from relevant areas. The development of the RAA should follow the following script:

1. Identification of assets related to the institution within the scope as described in section B;
2. Determination of threats that may be related to the Assets;
3. Identification of damage that can cause problems and compromise the security of information according to figure 03.
4. Use the following risk assessment methodology to categorize the identified menaces into four (04) broader categories: (a) Internal and accidental- Internal users' unintentional security breaches. (b) External and accidental- external users' unintentional security breaches (c) Internal and intentional- Intentional attacks from internal users and (d) External and intentional- willful attack by an external hacker. The possible sets of actions are shaded in each of the respective block to avoid these willful or accidental breaches (see figure 04).
5. Identify and scale the Vulnerabilities that can make the menace is emerging.
6. Describe the existing prevention of control to prevent damage.
7. Describe the controls before detection of threats to cause damage;
8. Document the SPW in the light of the identified risk-vulnerabilities and their occurrence and impact ;
9. Prioritize the risks of treatment with the SPW according to the academia's culture, value, beliefs and constraints to determine the implementation of controls that address risks;
10. Redo the RAA in accordance with the actions taken and use these in the existing SPW to formulate its new versions. While the Risk Assessment and Audit (RAA) will happen when following the cycles of SPW at least once a year at the moment of security incidents are identified.
11. And a report from RAA should be conducted with the approval of the High Direction and should be used with entry to the completion of treatment of risks i.e. incident handling and response.

3.5.6 Implementation of security Easy to Use Scheme

One of the major limitations of SITS approach is that people may find it difficult to use and thereby not to comply. Given the university community's apparent willingness to act securely if it proves convenient, institutions can take several approaches to make it easier for their users to behave in a secure fashion. Some of these are simple and low cost, where others require more effort to implement and maintain but also promise better returns. Because the more you make it easier for people to do the right things, the more successful you will be. These proposed approaches are enlisted below:

1. Create easy-to-follow instructions- to secure commonly used systems and applications and make them easily available on the Web.
2. Provide links of commonly used IT security tools such as antivirus software, personal firewall software, or secure communications tools like SSH or SFTP in an internal web site and making them easy to find and install.
3. The institution should create its own installers for commonly used operating systems and applications with all desired security modifications included and distribute them to campus system administrators and

Copyright (c) 2012 International Journal of Computer Science Issues. All Rights Reserved.

users on either an intranet server or physical media such as CDs.

4. Use automated system configuration tools to monitor individual systems' configurations and automatically push updates out to them as necessary.

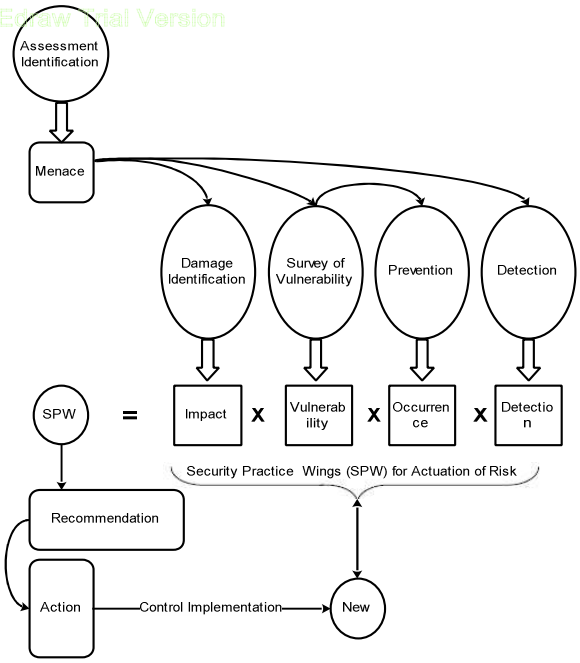

Fig 3: Risk Assessment and Audit (RAA)

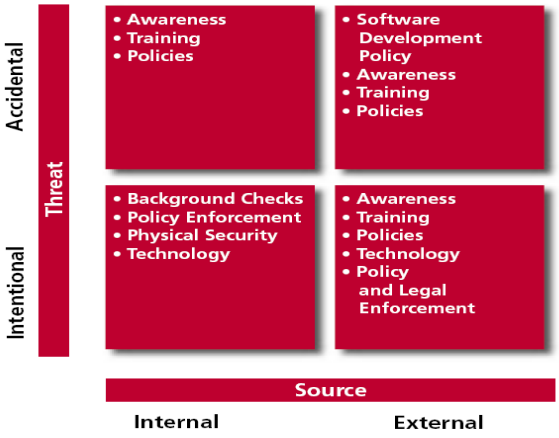

Fig 4: Risk Assessment Methodology

3.6 The RITS-B Approach

The proposed RITS-B approach is detailed in Roadmap 1. It consists of nine (09) steps those were grouped into three basic modules as discussed in section A, B and C to achieve the sustainability in the process of higher education secrecy and security for Muslim nations. An institution is defined by its value criterion as discussed above where its security challenges lies on its scope and scale- to assess the security concerns. The heterogeneous and diverse nature of institution and academia fuel the further processing needs of security in the domain of technology and generic soft interventions that is presented in section B and section C respectively. If the institutions are in the need of security then put the above mentioned nine steps under the same umbrella of secrecy where the institution's cultures, believes and values shows the further light towards the journey on robust security and sustainability in this complicated and insecure world environment.

Roadmap 01: Robust IT Security Balancing (RITS-B) Approach

Precondition: Institutions to be secured
Post condition: A more secured higher education environment

1. Define the institution's information security scope
   a. Develop a framework on fact and national perspective for campus security
   b. Identify security policies, tools, procedure and practices
2. Defining IT Security Strategic Assessment Scale
   a. Reactive
   b. Technology Centric
   c. Cultural
   d. Fortified
3. Document the institution's technological needs
   a. Technology/Tools vary
      i. with that of application and intrusions
      ii. with that of institutions wants, needs and abilities
   b. Main purpose: is to fulfill the requirements of (1) to (9) of section II
4. Model the Management System Information Security on campus
   a. Based on: DI-AI methodology
   b. Should follow the standards of NBR ISO/IEC-27001:2005
5. Model Information Security Organizational Structure
   a. Formulate a centralized office
   b. Decentralize it into ITPO and ITSO
   c. Have some dedicated staffs
6. Development of security plans and policies
7. Communication and awareness
8. Model the pattern of institutional IT Security Practices
9. Implementation of security Easy to Use Scheme

4 Quantitative Survey Result

In analyzing the security performance of the RITS-B approach, the responses of 6 senior university administrators- the majority of whom were Chief IT

Copyright (c) 2012 International Journal of Computer Science Issues. All Rights Reserved.

Officer and other director of CICT (Centre of Information and Communication Technology) /academic/administrative computing along with 66 academic personnel at 6 engineering institutions of Bangladesh were synthesized, from a June 2010 survey as reported in Information Technology Security Management in Engineering Universities in Bangladesh by Jahidul Arafat, Lecturer, University of Liberal Arts Bangladesh and Research Associate, HTRC, UK. The existing security trends of these institutions were queried by the respective researcher and in the light of the findings the RITS-B approach is developed and later the surveyed institutions were asked to implement this newly developed security scheme in their arena. The impact of the implementation status of this RITS-B approach at those institutions were further analyzed against three survey questions to assess respondents' opinions on the success of their IT security outcomes (Likert scale ranging from: 1= strongly agree, 2= agree, 3= Disagree, and 4= Strongly Disagree):

- How would you characterize your program success?
- Are data, network, and applications that are your responsibility secure?
- Is your institution more secure today than it was two years ago?

Table1. Impact of RITS-B'S implementation status over institution's IT security outcomes

Implementation Status of RITS-B Approach		IT Security Outcomes		
		Program is Successful	Systems are Secure	More Secure than 2 years ago
Fully Implemented	WA	-	-	-
	S.Div.	-	-	-
Partially Implemented	WA	2.25	1.75	1.25
	S.Div.	0.500	0.500	0.500
Didn't Implement	WA	3.50	3.00	2.50
	S.Div.	0.707	0.000	0.707
Scale: *1(Strongly Agree) = SA, 2(Agree) = A, 3(Disagree) = D and 4(Strongly Disagree)= SD.* N=6 (Institutions), WA= Weighted Average. S.Div.= Standard Deviation.				

And the table 1 shows that institutions which implemented the proposed RITS-B approach in their arena either fully or partially rate their IT security outcomes higher than those which didn't. This thereby dictates the significance of having this newly developed security model in the campus arena to gain robustness in the process of secrecy and security without violating the freedom and openness

5 Conclusion

The Soft IT Security (SITS) approach is a useful and important technique in higher education information security. In spite of its excellent persona such as simplicity, effectiveness and incident supervision, it is unable to achieve global optimum because of academic and departmental diversities and as because Muslim Ummah's interest and beliefs are not reflected here. On the other hand, the proposed Robust IT Security Balancing (RITSB) Approach considers the stages of Identification-Prioritization-Revision-Dynamicity for an acceptable use of soft security issues over the hard interventions and on the end user community while considering the academia's diversities, believes and constraints. In the RITS-B approach, the degree used for merging the hard and soft security concerns with that of the institution's belief, culture and constraints are derived dynamically based on similarity and value criterions of the regions and institutions. For these reasons, the RITS-B Approach is able to present the institution's security concerns from a holistic position. The quantitative survey results show that the institutions which had implemented this proposed security solution in their arena feeling more secure than two years ago. They also rated their system's security and program's success much higher than that of others. This increases the application area of the SITS approach where the robustness and dynamisms are needed.

References

[1] P. Arabasz, & J. Pirani, "Wireless networking in higher education", EDUCAUSE Center for Applied Research, Vol. 2, 2000, Available from: http://www.educause.edu/ecar/> [accessed 11 June 2010].
[2] B. Albrecht & J.B. Caruso. "Information Technology Security at Indiana University", Case Study, ECAR, 2003, No. 8.
[3] S. Bellovin, M. Blaze, E. Brickell, C. Brooks, V. Cerf, W. Diffie, S. Landau, J. Peterson & J. Treichler. "Security implications of applying the Communications Assistance to Law Enforcement Act to voice over IP", 2006.
[4] M. Dark, R. Epstein, L. Morales, T. Countermine, Q. Yuan, A. Muhammed, M. Rose & N. Harter, "A Framework for Information Security Ethics Education", 10th Colloquium

Copyright (c) 2012 International Journal of Computer Science Issues. All Rights Reserved.

for Information Systems Security Education- University of Maryland, 2006, 4, pp. 109-115.
[5] E.C. Ellen & M.A. Luker, "Finding the Will and the Way: Preparing Your Campus for a Networked Future", EDUCAUSE Leadership Strategies Series- San Francisco: Jossey-Bass Inc. Publishers, 2006, Vol. 1, pp. 85.
[6] EDUCAUSE, CALEA (Communications Assistance for Law Enforcement Act), [online], Available from:http://www.educause.edu/Browse /645?PARENT_ID=698, 2006, [accessed 21 August 2010].
[7] J. Fender, "LSU beefs up computer security. Capitol News Bureau" [online], 2006, Available from:<http://www.2theadvocate.com/news/3040126.html> [accessed 21 June 2010].
[8] T. Gray, Network Security Credo, [online], "EDUCAUSE Quarterly Publication",2005, 14(2), 12-14, http://staff.washington.edu/gray
[9] Executive Guide, "Information Security Management: Learning From Leading Organizations", 1998, GAO/AIMD-98-68.
[10] R.B. Kvavik & J. Voloudakis (with J.B. Caruso, R.N. Katz, P. King, & J.A. Pirani), "Information technology security: Governance, strategy, and practice in higher education", EDUCAUSE Center for Applied Research, 2003, Vol. 5, Available from: <http://www.educause.edu/ecar>
[11] J.A. Pirani, Sheep Pond Associates, J. Voloudakis, C.G. Ernst & Young, "Information Technology Security at MIT", Case Study, ECAR, 2003, No. 9.
[12] J.A. Pirani, Sheep Pond Associates & ECAR, "Incident response: Lesson Learned from Georgia Tech, the university of Montana & University of Texan at Austin", Case Study, ECAR, 2003, No. 7.
[13] A. Rivlin, "Circular No. A-123. Washington, DC: U.S. Office of Management and Budget", [online], 1995 Available: http://www.whitehouse.gov /OMB /circulars/a123/a123.html [21 August 2010].
[14] V.E., Rezmierski, D.M. Rothschild, A.S. Kazanis, & R.D. Rivas, "Final report of the computer incident factor analysis and categorization (CIFAC) project", 2005 Vol. 2, Available from: <http://www.educause.edu/ ir/library/pdf/CSD4455.pdf> [accessed 21 August 2010].
[15] D. Sieberg "Hackers shift focus to financial gain" [online], 2005 Available from: http://www.cnn.com/2005/TECH/internet /09/26/identity.hacker/index.html> [accessed 21 August 2010].
[16] J. Voloudakis & P. King, "Information Technology Security at the University of Washington", Case Study, ECAR, 2003, No. 10.
[17] Visa Inc, "Payment card industry data security standard", [online], 2004, Available: http://usa.visa.com/business/accepting_visa/ops_risk_management /cisp_merchants.html [21 August 2010].
[18] D. Ward, & B.L. Hawkins, "Presidential Leadership for Information Technology", EDUCASE Review, 2003, 38(3), 45.
[19] R. Yanosky & G. Salaway, "Identity management in higher education: A baseline study", EDUCAUSE Center for Applied Research, 2006, Vol. 2, Available from: http://www.educause.edu/ecar/

First Author: Jahidul Arafat is a full time faculty member of University of Liberal Arts Bangladesh in the Department of Computer Science and Engineering and Research Associate of HT Research and Consultancy, UK. He obtained his M.Sc. in Technical Education in Computer Science and Information technology from Islamic University of Technology (IUT), a subsidiary organ of OIC, Bangladesh in 2010 and BSc in Computer Science and Engineering from Military Institute of Science and Technology, Mirpur Cantonment, Bangladesh in 2008.. He is the author of two journal and three international conference papers in home and abroad. His research interest includes Image processing and information security especially at Network and policy level.

Second Author: Golam Moktader Daiyan is a full time faculty member of Southern University Bangladesh in the Department of Computer Science and Engineering. He obtained his M.Sc. Engineering in Computer Science and Engineering from Islamic University of Technology (IUT), a subsidiary organ of OIC, Bangladesh in 2011 and B.E in Computer Science and Engineering from Madurai Kamaraj University, India in 2004. His research interest includes Image processing, Computer Networks and Computer Security.

Third Author: Md. Waliullah has obtained his MSc Network & Computer Systems Security from University of Greenwich, London, UK in Dec 2010 and B.Sc. in Computer Science & Engineering from Hajee Mohammad Danesh Science & Technology University, Dinajpur, Bangladesh in Dec 2007. Also, He is a Cisco Certified Network Associate (CCNA). He is the author of two journals and one international conference papers. His research interest includes Wireless LAN security threats and Vulnerabilities, Intrusion Detection and prevention system, Secure Mobile IPV6 route optimization techniques, IT Governance and COBIT.

Copyright (c) 2012 International Journal of Computer Science Issues. All Rights Reserved.