IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 15, Issue 2 (Nov. - Dec. 2013), PP 30-34
www.iosrjournals.org

Recapitulating the development initiatives of a robust information security safeguard: RITSB-the proposed solution

Jahidul Arafat[1] and Md. Ahsan Habib[2]
[1]*Researcher, HT Research and Consultancy, UK.*
[2]*Department of Information and Communication Technology, Mawlana Bhashani Science and Technology University, Bangladesh*

Abstract: *Most current information security systems performance vary with the nature of the filed its being operating. With an increased emphasizes on the adoption of security tools and technologies, the anomalies and intrusion are mostly said defined to be detected on system's algorithm, when most systems have well defined mechanism for rapid reaction and identification of intrusions. However, despite this support for anomaly detection, this is usually limited and often require a full recompilation of the system to deploy a comprehensive framework of security governance, strategies and practices employing the policies in implementation.*

As a result, the absence of a robust security framework securing both the education and corporate resources has heightened the tension for a strategic information security solutions which might ends with cost, complexities and cumbersome to develop. This paper thereby presents an alternative comprehensive system namely RITS-B which accommodates both the nature of education and organizations without a need to for a further modification. Implication of the proposed approach at real time depicts its suitability in the arena of concern.

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

I. 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.

1.1 Structure of the study

This paper is organized as follows: the literature review related to the basic idea on higher education and corporate level IT security needs and various hard and soft aspects of security to secure their arena including their advantages and disadvantages is detailed in section 2. The RITS-B approach is presented in section 3. The quantitative survey results are provided in section 4 and finally section 5 shows some concluding remarks.

II. Literature Review

2.1 What if information 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
d) Scalability, scaling the belief of educational culture of one region from that of other regions and stimulate institution's interest to contribute in the field of information security concerns while preserving oaths and mandates of learning and knowledge sharing.

Thus the study can, in turn, characterize each of these seven protection categories: confidentiality, integrity, authenticity, scalability, non-repudiation, accountability, and availability-by levels of sensitivity: high (serious injury to an institution), medium (serious injury), and low (minor injury).

2.2 Hard and Soft Information security solutions

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 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.

2.3 Robust information security solution: rational to have

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.

All these are the pledge of the education and organization to gain success in openness and privacy in the field of information security.

III. Development initiatives of robust information security solution

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.

3.1 The RITS-B : The Proposed 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

IV. RITS-B implication at education and corporate level

In analyzing the security performance of the RITS-B approach, the responses of 6 senior university administrators- the majority of whom were Chief IT 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, 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 (both education and corporate organization) 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.				

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.

V. 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. 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]. Arabasz, P., & Pirani, J. (2002). Wireless networking in higher education, *EDUCAUSE Center for Applied Research,* Vol. 2, Available from: http://www.educause.edu/ecar/> [accessed 11 June 2010].

[2]. Albrecht, B. & Caruso, J.B. (2003). Information Technology Security at Indiana University, *Case Study, ECAR*, No. 8.

[3]. Bellovin, S., Blaze, M., Brickell, E., Brooks, C., Cerf, V., Diffie, W., Landau, S., Peterson, J., & Treichler, J. (2006). Security implications of applying the Communications Assistance to Law Enforcement Act to voice over IP.

[4]. Dark, M., Epstein, R., Morales, L., Countermine, T., Yuan, Q., Muhammed, Ali., Rose, M., & Harter, N. (2006). A Framework for Information Security Ethics Education. *10th Colloquium for Information Systems Security Education- University of Maryland*, 4, pp. 109-115.

[5]. Ellen E.C., & Luker M.A. (2000). Finding the Will and the Way: Preparing Your Campus for a Networked Future, *EDUCAUSE Leadership Strategies Series- San Francisco: Jossey-Bass Inc. Publishers*, Vol. 1, pp. 85.

[6]. EDUCAUSE. (2006). *CALEA (Communications Assistance for Law Enforcement Act)*, [online], Available from:<http://www.educause.edu/Browse /645?PARENT_ID=698> [accessed 21 August 2010].

[7]. Fender, J. (2006, June 13). LSU beefs up computer security. *Capitol News Bureau* [online], Available from:<http://www.2theadvocate.com/news/3040126.html> [accessed 21 June 2010].

[8]. Gray, T. (2005). Network Security Credo, [online], *EDUCAUSE Quarterly Publication,* 14(2), 12-14, http://staff.washington.edu/gray

[9]. Executive Guide (1998). Information Security Management: Learning From Leading Organizations, *GAO/AIMD-98-68*, May.

[10]. Kvavik, R. B., & Voloudakis, J. (with Caruso, J. B., Katz, R. N., King, P., & Pirani, J. A.). (2003). Information technology security: Governance, strategy, and practice in higher education, *EDUCAUSE Center for Applied Research,* Vol. 5, Available from: <http://www.educause.edu/ecar>

[11]. Pirani, J.A., Sheep Pond Associates, Voloudakis, J., Ernst, C.G. & Young. (2003). Information Technology Security at MIT, *Case Study, ECAR*, No. 9.

[12]. Pirani, J.A., 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.
[13]. Rivlin, A. (1995). Circular No. A-123. *Washington, DC: U.S. Office of Management and Budget,* [online], Available: http://www.whitehouse.gov /OMB /circulars/a123/a123.html [21 August 2010].
[14]. Rezmierski, V. E., Rothschild, D. M., Kazanis, A. S., & Rivas, R. D. (2005). *Final report of the computer incident factor analysis and categorization (CIFAC)* project, Vol. 2, Available from: <http://www.educause.edu/ ir/library/pdf/CSD4455.pdf> [accessed 21 August 2010].
[15]. Sieberg, D. (2005, September 26). *Hackers shift focus to financial gain* [online], Available from: <http://www.cnn.com/2005/TECH/internet /09/26/identity.hacker/index.html> [accessed 21 August 2010].
[16]. Voloudakis, J. & King, P. (2003). Information Technology Security at the University of Washington, *Case Study, ECAR*, No. 10.
[17]. Visa Inc. (2004, December 15). *Payment card industry data security standard* [online], Available: http://usa.visa.com/business/accepting_visa/ops_risk_management /cisp_merchants.html [21 August 2010].
[18]. Ward D., & Hawkins B.L. (2003). Presidential Leadership for Information Technology. *EDUCASE Review,* 38(3), 45.
[19]. Yanosky, R. & Salaway, G. (2006). Identity management in higher education: A baseline study, *EDUCAUSE Center for Applied Research*, Vol. 2, Available from: http://www.educause.edu/ecar/