Information Technology Security, Strategies and Practices in Higher Education: A Literature Review

Md. Waliullah, Jahidul Arafat, Golam Moktader Daiyan

Abstract—Information security is a feverish issue 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 Balanced (composition of Technical and Non-technical security issues) IT Security approach (BITS) is highly lucrative now-a-days due to its simplicity and effectiveness in the sector of Information security especially in Higher education. Numerous researchers have performed their research work on this approach to triumph over its limitations for its sustainable and component implementation This paper has consolidated the useful consideration and proposal of various researchers to formulate a strong base of knowledge for the future researcher. It has also tined few unsettled issues of BITS approach which will open the casement of brainstorming as well as persuade them for future research on BITS approach, thereby allow BITS approach to attain a globally satisfactory shape for higher education information security

Index Terms—: Information security, Hard Intervention, Soft intervention, balanced approach, Strategy, Practice.

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 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

- *Md. Waliullah is with the School of Computing & Mathematical Sciences, University of Greenwich, London, United Kingdom..*
- *Jahidul Arafat is with the Technical and Vocational Engineering Department, Islamic University of Technology, Bangladesh.*
- *Golam Moktader Daiyan is with the Computer Science and Information Technology Department, Southern University Bangladesh*

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. Some frameworks on it are detailed in Ellen & Luker (2000), Kvavik & Voloudakis (2003) and Yanosky & Salaway (2006). 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.

Several papers (Bellovin et al, 2003; EDUCASE, 2006; Fender, 2006; Rivlin, 1995; Ward & Hawkins, 2003) are now available which highlight and describe various techniques of soft IT interventions to overcome difficulties/limitations of only having the hard interventions. In this paper, the second approach i.e., soft security aspects are generalized with its basic features, the advantages, shortcoming as well as various techniques to overcome few of those shortcomings in the field of higher education security solution. We have emphasized on frameworks proposed by Arabasz & Pirani (2002), Kvavik & Voloudakis (2003) and Yanosky & Salaway (2006) throughout this paper for describing balanced security solutions.

This paper is organized as follows: in section 2, the basic idea on higher education IT security including their advantages and disadvantages are described while few techniques for overcoming the drawbacks of security balancing scheme are presented in Section 3. Finally, some concluding remarks are given in Section 4.

2 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):

- Confidentiality or protection from unauthorized use or disclosure of information.
- Integrity, ensuring data accuracy and completeness through protection from unauthorized, unanticipated, or unintentional modification, and including authenticity and
- Availability, making data available to the authorized users on a timely basis and when needed.

We can, in turn, characterize each of these six protection categories: confidentiality, integrity, authenticity, nonrepudiation, accountability, 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 to ensure such level an institution have two choices: either to follow the security approach (a) or (b) as mentioned in section 1 or go for the use of a blended approach- balancing the features of (a) and (b) according to its academia's needs and resource constrains to foster the institution's security goal. Where this balancing scheme requires the exploration of the following issues:

1) Make IT security a priority;
2) Selecting security controls and products
3) Defining and empowering acceptable behavior [by students, faculty, and staff];
4) Revise instructional security policy and improve the use of existing security tools;
5) Making consistent, timely, and cost-effective management decisions.
6) Improve security for further research and education networks;
7) Integrate work in higher education with national effort to strengthen critical infrastructure. And
8) Empowering [members of the institution's community to do their work] securely.
9) And all these are the pledge of the higher education to gain success in openness and privacy in the field of information security.

Security Management by Hard/Soft Interventions

1) Balancing IT security approaches by 'Hard' interventions is a procedure that groups the technological requirements and academia's 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):

1) Academia's resource and budgetary constrains
2) IT security does not appear to be high on most institutions' executive agenda.

3) The "transient" nature of the higher education's constituents complicates the IT security management.
4) The rapid changing nature of the intrusions.
5) 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.

2.1 Security Management By Hard and Soft Interventions

An alternative of the previous methods consists of initially having a look on what types of security tools academia is currently having and then try to determine a soft layout on them to determine 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: Technology i.e. security tools, Policies, Awareness, Leadership and Practices.

The calculation of all of these features involves the topology of the academia's nature and ability. There is also a sixth requirement involving a hierarchical organization as follows:

Find the academia's values and believes which has produced the requirements of the above fives and other consequent security requirements generated by these ethical concerns.Based on the use of the technological and cultural aspects Kavavik & Voloudakis (2003) have suggested four major strategies or approaches (Figure 1) for securing an educational institution on the basis of the institution's strength in each arena. And these are: **(i)** Reactive **(ii)** Cultural **(iii)** Technology Centric and **(iv)** Fortified.

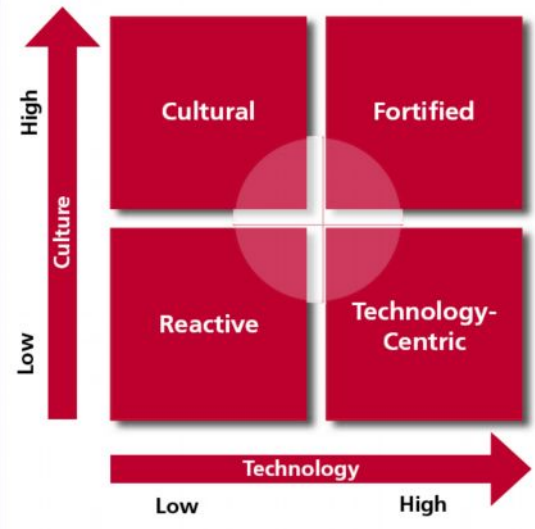

Fig.1. IT Security Approach

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.

3 Modification on BITS Techniques

Several techniques already introduced to modify the higher education IT security approaches which are detailed in the next sections. These security balancing and modification processes are summarized as follows to fulfill the requirements of (1) to (8) of section 2.

- Identify the exiting higher education environment.
- Prioritize the IT security issue around the academia and administrative arena.
- Revise instructional security governance, strategy and practices and improve the use of existing security tools.
- Keep the paces with the educational and environmental changes rather being to be conclusive.

3.1 Robust Technology Selection

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 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 (Rezmierski, Rothschild, Kazanis & Rivas, 2005). The ultimate goal is to fulfill the requirements of (1) to (8) of section 2.

3.2 Measurement of Soft Security Feature

A standard higher education environment is described by its soft properties. A higher education environment is said to be secured if it satisfies the requirements of (b) - (f) of section 2.2. These soft properties basically define a non-technical security model. Various soft property measurement criterions are discussed in the following sections to modify the above proposed security balancing scheme.

3.3 IT Security Management on Campus

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 don't prove knowledge but shows that you putted your time and effort to gain the specialized skill (Kvavik & Voloudakis, 2003). The salary trends of these IT security personnel are further queried by Sieberg (2005) and Visa Inc. (2004).

3.4 IT Security Organizational Structure

Absence of a robust security organizational structure may hinder the security implementation. Several IT security literatures (Kvavik & Voloudakis, 2003; Yanosky & Salaway, 2006) recommend the establishment of a central security office where Government Accounting Office (GAO) in its 1998 Executive guide had pointed out the ways through which central security offices can help the institution. Moreover, institutions with a dedicated security staff are much more likely fulfill these functions. Several survey papers (Albrecht & Caruso, 2003; Pirani, Sheep Pond Associates, Voloudakis, Ernst & Young, 2003; Voloudakis & King, 2003) provide examples of such organizational structures. Indiana University (IU) established two distinct offices: the Information Technology Policy Office (ITPO) and the Information Technology Security Office (ITSO). These offices are intentionally distinct: the ITPO handles IT policy development, dissemination, and education, and the ITSO handles security analysis, development, education, and guidance for IU's information assets and IT environment. A similar or somehow different pattern is exists in South Dakota State University and Yale University.

3.5 Security Policy

A significant drawback of BITS approach is that it may inhibit the academic freedom by limiting access to certain information. To solve this problem another measure which operates on the soft-security level is the security policy derivation, codification and implementation. The idea is to consider the value criteria of a particular educational institution where Institutional values drive policy and policy thereby dictates processes, procedures, and standards; and security implements those (Executive Guide, 1998).

Several IT security literatures (Kvavik & Voloudakis, 2003; Albrecht & Caruso, 2003)) recommends on the characteristics of these security policies: Policy should be (a) accessible (b) clear and easy to read (c) consistent across the institution (d) enforced (e) regularly updated and (f) comprehensive. Where security policies provides a framework for (a) making consistent, timely, and cost-effective management decisions; (b) selecting security controls and products; (c) defining and empowering acceptable behavior from users; and (d) to work securely (Yanosky & Salaway, 2006).

IT security policy not only supports academic freedom but also ensure ready and timely access to information to authorized users and thereby preserve academy's most important values into an area that some might otherwise find problematic. A good security policy can play an important role in liability abatement by demonstrating that the institution has taken appropriate and necessary precautions to protect its information assets.

3.6 Senior Management's Involvement in Policy Development

Senior managements' negligence on IT security can hinder the progress of BITS approach. The best-practice literatures (Kvavik & Voloudakis, 2003; Ward & Hawkins, 2003) on policy development encouraged that IT security discussions need to be conducted in layman's terms and focus on its impact on users as much as, and perhaps more than, its impact on the institution. And the discussion should involve representatives from all sectors of the institution and should be done periodically.

3.7 Awareness

A policy cannot be effective by itself. Neither it nor the IT security organizational structure produces a subjectively appropriate security until there are some awareness programs regarding these. 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 (Arabasz & Pirani, 2002; Yanosky & Salaway, 2006). 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 de gree of awareness. Awareness building does not have to cost a lot of money, but it definitely needs attention (Kvavik & Voloudakis, 2003).

3.8 Security Planning

Although the above fives handles well most security aspects those occurs in an educational environment. But the effective use of security technologies depends on Information Technology (IT) security practices where achievement of a generalized security solution is one of the major limitation of BITS. For these, institutions' need to have either any of the followings three planning scheme in their place (Yanosky & Salaway, 2006): (a) A comprehensive plan (b) Partial plan or (c) Currently developing plan.

3.9 IT Security Practices

Risk Assessments and Audits

Risk assessment helps an institution to determine its security requirements while periodic reviews are necessary to accommodate changes to the institution's academic activities and business operations, to account for new threats and vulnerabilities, and to confirm that current controls are effective and operative (Gray, 2005).

Kvavik & Voloudakis (2003) have suggested the following risk assessment methodology (Figure 2) which is capable to address the four different risk 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. They also recommend for the development of a business case for institutions' IT security to profiles and compare risks and effectively present them to non-technical management.

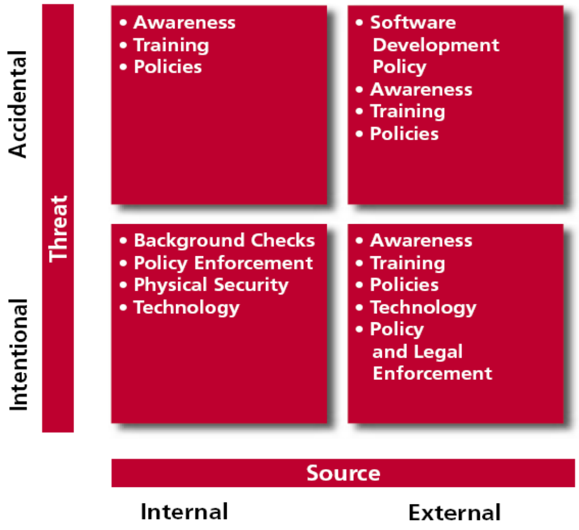

Fig.2. Risk Assessment and Response

Although this model is a good one to balance security technologies with that of cultural aspects but is less effective against accidental ones. Similarly, cultural tools such as policies, procedures, and awareness provide a strong defense against accidental exposures and complement technology to provide a stronger defense against intentional threats.

Updating and Maintaining Systems

Another aspect of IT security practices is not only maintains but also updates the campus wide security system. Kvavik & Voloudakis (2003) pushed emphasizes on that all new enterprise systems and applications (a) should be tested for IT security and (b) also should be certified for IT security.

Access Control Procedure and Detection-Monitoring Process

Well defined control procedures and processes performed by hardware, software and administrators helps the institution to: (a) monitor access (b) identify users requesting access (c) record access attempts (d) only allow authorized person/program to access to system's resources And (e) routinely terminate e-mail, network and other enterprise systems accesses. Moreover, periodic changes on institutions' key enterprise systems and a well defined procedure for identifying users before resetting passwords, tokens and PINs can ensure the further securities. Institution should have monitoring schemes for its user accounts, network, operating system, enterprise system, routers and should execute this scheme periodically (Dark et al, 2006; Rivlin, 1995).

Incident Response Scheme

To mitigate the most possible cyber attacks for many institutions, being a good "Net citizen" and preventing the use of institutional resources from such attacks is nearly as high a priority as protecting their own information.

Since the creation of the first worm by Robert Tappan Morris (Cornell University graduate student) in 1988 security breach attempts are now a daily reality for the higher education institution. Several papers (Pirani, Sheep Pond Associates & ECAR., 2003; Voloudakis & King, 2003) have reported such kind of breach incidents in higher education.

The University of Washington's Terry Gray classifies these threats in seven categories where each has been a reality for higher education (Voloudakis & King, 2003). (a) Application level security threats (b) threats to network infrastructure devices (c) threats to core network computing services (d) theft of network connectivity services by unauthorized users; (e) unauthorized access to hosts via the Internet;

(f) unintended disclosure or modification of data sent between hosts; and (g) Denial -of-service attacks against connected hosts. Now, to avoid and overcome from such problems institutions should have the following factors in place: (a) presence of a robust security architecture (b) a comprehensive security policy and continual security education and training (c) a formal IT security handling procedure. (b) a significant Macintosh presence on campus; (c) implementation of port blocking, (d) availability of virtual private network (VPN) service as an alternative (e) Proactive scanning and effective intrusion detection and (f) Centralized and other mechanism for alerting users about such threats and intrusions (Arabasz & Pirani, 2002; Rezmierski, Rothschild, Kazanis & Rivas, 2005). Yanosky & Salaway (2006) further suggested that, border blocks plus VPNs appeared to be the most effective and desirable practice for minimizing this worm's impact on end users.

Easy to Use Scheme

One of the major limitations of BITS approach is that people may find it difficult to use and thereby to cope up. 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 (Kvavik & Voloudakis, 2003). These approaches are enlisted below:

Approach 01: Create easy-to-follow instructions- to secure commonly used systems and applications and make them easily available on the Web.

Approach 02: 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.

Approach 03: 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 users on either an intranet server or physical media such as CDs.

Approach 04: Use automated system configuration tools to monitor individual systems' configurations and automatically push updates out to them as necessary.

By implementing one or more of these suggested approaches and lowering the barriers for users and departments to make them more secure, institutions increase the likelihood that their community will make more of an effort to secure their systems and applications, increasing the level of security for the institution as a whole.

4 CONCLUSION

Balanced IT Security (BITS) 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 has few limitations also. The initial BITS approach as proposed by Kavavik and Voludakis (2003) are tailored and enhanced upon by various researchers to eradicate few of its limitations. Their efforts have bought this approach into a formidable and significant standard at present. But the well-recognized globally optimal solutions to its problem could not be achieved due to institutions inherent dynamic nature. Endeavor of this, this paper will encourage IT people along with the administrative personnel to look eagerly into this aspect and in future the BITS approach will be able to triumph over a better stable, widely recognized and dynamically applicable in all types of educational environment. The problem specification of this paper will act as the centre point of the researcher's innovation and analysis of different existing techniques will assist them being a knowledge hoard in their progress of research work.

REFERENCES

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

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

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

[5] E.C. Ellen, & E. C. Luker (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. 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].

[6] J. Fender, (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].

[7] T. Gray, (2005). "Network Security Credo", [online], *EDUCAUSE Quarterly Publication,* 14(2), 12-14, http://staff.washington.edu/gray Executive Guide (1998). Information Security Management: Learning From Leading Organizations, *GAO/AIMD-98-68*, May.

[8] R.B Kvavik, & J. Voloudakis, (with J. B. Caruso, R. N. Katz, P. King, & J. A. Pirani,). (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

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

[10] J. A. 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.

[11] A. Rivlin, (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].

[12] V. E. Rezmierski, Rothschild, D. M., A. S. Kazanis, & R. D. Rivas, (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].

[13] D. Sieberg, (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].

[14] J. Voloudakis, & P. King, (2003). "Information Technology Security at the University of Washington", *Case Study, ECAR*, No. 10.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].

[15] D. Ward , & B. L. Hawkins (2003). Presidential Leadership for Information Technology. *EDUCASE Review,* 38(3), 45.

[16] R. Yanosky, & G. Salaway, (2006). "Identity management in higher education: A baseline study", *EDUCAUSE Center for Applied Research*, Vol. 2, Available from: <http://www.educause.edu/ecar/>

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.

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.

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.