IT Security In The Higher Education Institutions

Dave E. Marcial[1]
demarcial@su.edu.ph

Abstract

This paper investigates the level of prioritization and degree of implementation of IT security in higher education institutions (HEIs) in the Philippines. A total of 95 HEIs in the Philippines were evaluated in the study. The study reveals that the level of prioritization of IT security in the Philippines HEIs is high. This signifies that IT security is prioritized and there is need to be done in the next 3 years in these HEIs. The degree of implementation of IT security in the HEIs is moderately implemented indicating that although this component is in the strategic plan of the HEIs, little or no action has been undertaken in this regard. The study further reveals that the level of prioritization of IT security has a significant correlation at 0.01 level of confidence with the degree of implementation of IT security in the HEIs in the Philippines.

Keywords : security, privacy, risk, IT in education

1. INTRODUCTION

In this ever changing world where complex systems are rapidly evolving, everyone is always seeking for the outmost security. Webster defines security as quality or state of being secure that measure taken to guard against espionage or sabotage, crime, attack, or escape. It refers to the degree of protection against danger, damage, loss, and crime. It takes into account the actions of people attempting to cause destruction. The Asia-pacific region faced with the challenges that lie mainly in the general lack of awareness of IT security issues (Sembok, 2003).

Among the many realm of security is information technology (IT) that particularly focuses on application, computing, data, network, information, and among others. The purpose of IT security is to formulate methods to prevent the weaknesses from being exploited on the three important aspects of any IT-related systems: the confidentiality, integrity, and availability. The three broad categories of system resources (hardware, software, and data) and the connections among them are all potential security weak points (Pfleeger & Pfleeger, 2003).

[1] *College of Computer Studies, Silliman University, Dumaguete City, Philippines*

However, even how secure an IT-related system is, anyone can develop attacks and destroy its vulnerabilities. There are four kinds of attacks on IT systems, these are: interception, interruption, modification, and fabrication (Pfleeger & Pfleeger, 2003). Reports show significant events that destroy vulnerabilities of IT-related systems. In UK, the cases of information security breaches are on the rise because businesses have begun to operate differently and now depend more on technology (Shukla, 2010). In Malaysia, there are 394 incidences of cybercrime in the first six months of 2003; in Japan, crime related to internet dating services more than doubled in the first six months of 2002; in South Korea, cyber offences shot up 126 percent (33,289 cases) in 2001 from a year before; in Hong Kong, cybercrimes from 1995-2000 has an increase from a total number of 14 in 1995 to 368 in 2000, an increase in 26 times in 5 years (Sembok, 2003). In the Philippines, four people hacked into the accounts of AT&T business customers in the United States (Sengupta, 2011). In the article of Computerworld Philippines, the stable growth of cybercrime had an adverse effect among social networking sites users particularly on the confidence and trust issues. In the same article, it was cited that RSA, the security division of EMC corporation, revealed a survey that consumers are now more aware of phishing threats, but new attack methods duped six times as many in just two years.

While the business sectors are experiencing rampant IT security breaches, reports also show that the educational institutions are also facing constant growth of IT security problems. EDUCAUSE reported that IT security is 4th in rank among the 2011 top 10 IT-related issues in the higher education institutions (Ingerman, Yang and the 2010 EDUCAUSE Current Issues Committee, 2010). Moreover, EDUCASE revealed that IT security is at #1 or #2 on the list of “potential to become more significant in higher education institutions in the coming year". The result, according to EDUCASE, implies that we still haven't seen the whole scope of either the challenge or the solution. The following excerpts are descriptions by EDUCAUSE on its survey on 2011 Top-Ten IT Issues, as follows:

> *The security arms race continues, with hackers repeatedly finding ways to defeat the best technical, organizational, and social countermeasures created by security experts. We are seeing new exploits that automated intrusion detection fails to recognize, malware that is difficult to remove, and whole new waves of risk associated with the rapid deployment of smartphones and the new generation of tablets on institutional networks. We are drawn, both institutionally and individually, to cloud computing and other alternative sourcing arrangements with new and poorly understood security characteristics.*

> *Large releases of personally identifiable information (PII) and their aftermath continue to be regular features of the landscape for educational institutions. Institutional leaders, faculty, staff, students, parents, politicians, donors, and taxpayers all demand, quite understandably, to know how educational institutions are going to address the problem. News coverage of these breaches brings both challenges and, oddly, a bit of help: on the one hand, the coverage raises expectations among our users for security and privacy efforts; on the other hand, the constant exposure makes it easier to raise campus awareness of the risks involved with inaction.*

In the Philippines Business Guide produced by the UK Trade & Investment, the Philippines has a well-developed network of communications infrastructure that connects the three largest island groups of Luzon, Visayas and Mindanao. Its specialized IT zones provide computer security and building monitoring systems. The Commission on Higher Education (CHED), an attached agency to the Office of the President of the Philippines for administrative purposes, formulates and recommends development plans, policies, priorities, and programs on higher education. The total higher education institutions (HEIs), based on the list published on December, 2010 in the CHED's website is 1,496; 112 of which are public colleges and universities and 1,384 are private colleges and universities.

This paper investigates the level of prioritization and degree of implementation of information security in higher education institutions in the Philippines. Prioritization as used in this study refers to the level of importance or urgency of IT security in the HEIs while implementation refers to the degree of realization or execution of IT security in HEIs in the Philippines. This paper also demonstrates the relationship between the level of prioritization and degree of implementation of IT security in higher education institutions in the Philippines. It further demonstrates the significant differences between the level of prioritization and degree of implementation of IT security in higher education institutions in the Philippines in terms of the: total number of years of existence of the HEIs; annual IT expenditures of the total Internet bandwidth of the HEIs; level of proficiency of the respondent's technical skills; rating of the respondents' human skills; rating of the respondent's conceptual skills; and extent of participation in decision-making of the respondents.

2. METHODOLOGY

This paper is a derived document from the study on the landscape of IT in the HEIs in the Philippines. The study was a descriptive-correlative and utilized a survey method. The respondents of the study are all higher education institutions in the Philippines. Only one respondent per HEIs is allowed to participate in the survey. He/She must be the IT Manager or the person in-charge of the management information systems or IT-related services in the HEIs.

During the administration of the study, a sample size of the respondents was determined where the total number of population (N) was based on the list of HEIs published in the official website of CHED. In this case, the total HEIs based on the list is 1,496; 112 of which are public colleges and universities and 1,384 are private colleges and universities. The sample size was rounded off to 316 HEIs. Computation of the sample size is as follows:

$$n = \frac{N}{1 + Ne^2} \quad [1]$$

where n is the sample size, N is the total population and e is the margin of error. A 5% margin of error is used in the study. Using the stratified sampling procedure as computed below

$$\% = \frac{n}{N} \quad [2]$$

A total of 316 HEIs in the Philippines was included in the survey. Respondents per region in the Philippines were identified randomly using a computerized random number generator (Weaver & raulin, 2007). See appendix for the Philippine map to locate the regions.

Table 1.
Respondents' Regional Distribution

Regions in Philippines	Public	Private	Total HEI-Respondents
1 (locos Region)	1	3	4
2 (Cagayan Valley)	0	5	5
3 (Central Luzon)	1	4	5
4 (Calabarzon)	1	3	4
5 (Bicol Region)	3	3	6
6 (Western Visayas)	1	11	12
7 (Central Visayas)	1	17	18
8 (Eastern Visayas)	2	4	6
9 (Zamboanga Peninsula)	0	5	5
10 (Northern Mindanao)	1	1	2
11 (Davao Region)	2	6	8
12 (Soccsksargen)	0	4	4
13 (National Capital Region)	0	9	9
14 (Cordillera Administrative Region)	0	2	2
15 (Autonomous Region of Muslim Mindanao)	0	1	1
16 (Caraga)	0	2	2
17 (MIMAROPA)	2	0	2
TOTAL	15	80	95

A total of 97 HEIs participated during the administration of the survey, two of which were disqualified due to the qualification of the person who answered the survey questionnaire. A total of 14 HEIs formally signified not to participate in the survey and two sets of questionnaires were returned via the post office due to address not found. Table 1 presents the regional distribution of the HEIs qualified in the survey. Of the 95 HEIs that were evaluated, 15 are public colleges and universities and 80 are private colleges and universities.

2.1 The Instrument and its Administration

The instrument used in data gathering to accomplish the specific objectives of the study was a researcher-made survey questionnaire. The survey questionnaire is composed of close-ended questions that are based on the critical questions that EDUCAUSE has pointed out in the 2010 top IT issues in higher education, particularly on the critical questions concerning security. Respondents were asked to evaluate the level of prioritization according to the five alternative choices: 1-Not a priority, 2-Low priority, 3-Medium priority, 4-High priority, and 5-Essential. Likewise, respondents were asked to evaluate the degree of implementation of each IT component according to the five alternative choices: 1-Not Implemented, 2-Fairly Implemented, 3-Moderately Implemented, 4-Highly Implemented, and 5-Very Highly Implemented.

The survey administration process is limited to four administrations. The first administration was done by sending the questionnaire through the email addresses of each respondent as published by CHED in its website on February 4, 2011. The second administration was done personally to some identified respondents who attended the 2011 National Convention of the Philippine Society of IT Educators held February 16-19, 2011 in Antipolo City, Manila, Philippines. The third administration was done on March 4, 2011 by sending a printed copy of questionnaires addressed to the school heads. The fourth administration was done by sending the electronic questionnaire through email directly to some of the identified respondents (IT managers or related position).

Follow–up processes were also limited through making telephone call and sending text messages to the respondents who did not respond based on the indicated deadline. Telephone numbers were based on the list published in the CHED website. A weekly follow-up through email was also done to have a greater participation from the HEIs. Only those HEIs who sent back the filled-up questionnaire from February 4, 2011 to April 30, 2011 were included in this study.

3. RESULTS AND DISCUSSION

3.1 The Prioritization of IT Security in the Higher Education Institutions in the Philippines

According to Associated Press, universities and colleges are prime targets of security attacks because universities and colleges repeatedly operate and run systems with vulnerabilities and few monitoring activities as explained by Richard Power, editorial director for the Computer Security Institute (Pfleeger & Pfleeger, 2003). Likewise, the National Center for Education Statistics of the US Department of Education pointed that while computers and networks contribute to the efficiency of educational record-keeping, data access, and use, they have not changed the reasons schools need to maintain, share, and use student and staff information. On the other hand, as security threats grow in severity and as institutions continue to face limited resources to combat them, it seems likely that security will remain a top concern for higher education for years to come institutions (Ingerman, Yang and the 2010 EDUCAUSE Current Issues Committee, 2010). This may imply that HEIs need to consider IT security to be one of the top priorities.

The level of prioritization of IT security in the HEIs in the Philippines (Table 2) shows that the aggregate mean of IT security in the higher education institutions in the Philippines is 3.80, which has the description of high priority. This signifies that IT security in the HEIs is prioritized and there is need to be done in the next 3 years. Likewise, the highest weighted mean of the items in IT security is 4.20 which is essential and this is on the item that the "institution should have a written privacy and security policies." This indicates that this item is already in place in the respondents' HEIs. The result may signify also that HEIs in the Philippines are highly protecting their information as it (information) is the lifeblood of any educational institution. Educational institutions collect, process and store information about their resources, activities and other stakeholders. This information can be described about students, faculty, staff, degree courses and programs, facilities, activities and other operations in the institution, as explained by National Center for Education Statistics of the US Department of Education. All these are collected and maintained so that schools can effectively organize services offered to students, measure learning progress, assign and monitor staff responsibilities and resource use, and provide other valued services to their communities.

Further, the study also reveals that the private HEI's level of prioritization is better ($\bar{x}$ = 3.85) compare to the public HEIs in the Philippines ($\bar{x}$ = 3.53). When the respondents are grouped according to gender, the data shows that the male IT managers have better weighted mean (3.83) of their level of prioritization of IT security than the female ($\bar{x}$ = 3.80). When grouped according to civil status, the study reveals that both single and

married IT managers have the same weighted mean of their level of prioritization of IT security which is 3.82. When the respondents are classified according to highest educational attainment, those who have doctorate degree have the highest weighted mean (3.89) of their level of prioritization of IT security compare to those with bachelor's degree ($\bar{x}$ = 3.64) and master's degree ($\bar{x}$ = 3.85). Lastly, IT managers who are working as fulltime have better weighted mean of level of prioritization of IT security (4.02) than the part-time IT managers with only $\bar{x}$ = 3.62.

Table 2.
Level of Prioritization of IT Security in the HEIs

Items on IT Security	Weighted Mean ($\bar{x}$)	Description
1) The institution should have a written privacy and security policies	4.20	Essential
2) The institution should have an aggressive program of data encryption particularly for data handled and carried by staff with legitimate access to secure and personal data	3.73	High Priority
3) The institution should identify firms and consultants who can be hired to assess and help implement the forensics capability that needs to be in place to analyze breaches and help prevent them in the future	3.26	Medium Priority
4) The institution should have adequate staff for security to address the security agenda particularly to assess the risks to, and ensure the privacy and security of, the institution's information resources	3.80	High Priority
5) The institution should view IT security as a funding priority	3.75	High Priority
6) The institution should plan or implement a comprehensive risk assessment to identify and prioritize vulnerable areas and outline ways to mitigate potential risks	3.75	High Priority
7) The institution should routinely consider privacy and security implications before buying or deploying new systems or technologies	3.95	High Priority
8) The institution should provide an awareness and training program in privacy and security that includes awareness of the defensive measures appropriate to the institution to protect systems and data	3.90	High Priority
9) The institution should implement a unified threat and vulnerability management system that includes such features as firewalls, VPNs, antivirus, antispyware, antispam and antiphishing, bandwidth management, intrusion prevention and detection, and content filtering	4.08	High Priority
10) The institution should participate in leveraging local, national, and global information security communities and resources.	3.55	High Priority
Aggregate Mean	3.80	High Priority

3.2 The Implementation of IT Security in the Higher Education Institutions in the Philippines

Despite of the increasing security issues in school, universities and colleges are implementing security measures. Huang Ee Choon, deputy director of the National University of Singapore's computer center, cited by (Tsang, 2007), pointed out that because the university is keeping "critical and sensitive resources" readily available in a digital format, additional security measures should be implemented.

The degree of implementation of IT security (Table 3), has an aggregate mean of 2.97 with a description of moderately implemented. IT security is in the HEI's strategic plan but there is no action that it has been done. Highly implemented item of IT security is item 1 indicating that development of a written privacy and security policies is continuing and on-going. This is unlike with the survey conducted in 1996 adapted from Snapshot, cited by (O'Brien, 1999), on the weaknesses in safeguarding proprietary information, where 49% of the respondents indicated that they have no written policies for information systems' security. The result provides a good indicator that the HEIs in the Philippines are ready to face many business control and security challenges (Frenzel, 1999). However, identifying firms and consultations for possible hiring of consultant is the least degree of implementation on IT security among the respondents with fairly implemented rating. This indicates that this item of IT security is discussed and considered for inclusion in the next strategic plan of the HEIs.

Table 3.
Degree of Implementation of IT Security in the HEIs

Items on IT Security	Weighted Mean ($\bar{x}$)	Description
1) The institution has a written privacy and security policies	3.45	Highly Implemented
2) The institution has an aggressive program of data encryption — particularly for data handled and carried by staff with legitimate access to secure and personal data	2.82	Moderately Implemented
3) The institution identifies firms and consultants who can be hired to assess and help implement the forensics capability that needs to be in place to analyze breaches and help prevent them in the future	2.42	Fairly Implemented
4) The institution has adequate staff for security to address the security agenda particularly to assess the risks to, and ensure the privacy and security of, the institution's information resources	2.95	Moderately Implemented
5) The institution views IT security as a funding priority	2.86	Moderately Implemented
6) The institution plans or implement a comprehensive risk assessment to identify and prioritize vulnerable areas and outline ways to mitigate potential risks	2.88	Moderately Implemented

Table 3.
Degree of Implementation of IT Security in the HEIs (cont')

7) The institution routinely considers privacy and security implications before buying or deploying new systems or technologies	3.14	Moderately Implemented
8) The institution provides an awareness and training program in privacy and security that includes awareness of the defensive measures appropriate to the institution to protect systems and data	3.03	Moderately Implemented
9) The institution implements a unified threat and vulnerability management system that includes such features as firewalls, VPNs, antivirus, antispyware, antispam and antiphishing, bandwidth management, intrusion prevention and detection, and content filtering	3.35	Moderately Implemented
10) The institution participates in leveraging local, national, and global information security communities and resources.	2.77	Moderately Implemented
Aggregate Mean	2.97	Moderately Implemented

The result also suggests that IT support for the HEI' administrative process and academic teaching in the Philippines is at certain moderation. According to Attipa Julpisit, cited by (Tsang, 2007), IT serves as a primary support to both the university's administrative process and academic teaching. Among these that need to be secured include: Communication Support Systems (CSS), Transactional Processing Systems (TPS), Office Automation Systems (OAS), Management Information Systems (MIS), Decision Support Systems (DSS), and Executive Information Systems (EIS).

The aggregate mean of the degree of implementation of the IT security presented in the study shows that all these components are already implemented but no action has been established to achieve these components. However, according to the result on the level of prioritization, the aggregate mean of IT security is highly prioritized and need to be done by the HEIs in the next 3 years.

Further, the study also reveals that the private HEI's level of implementation of IT security is better ($\bar{x}$ = 3.05) compare to the public HEIs in the Philippines ($\bar{x}$ = 2.55). When the respondents are grouped according to gender, the study reveals that the male IT managers have better weighted mean (2.97) than the female (2.95) of their level of prioritization of IT security. When grouped according to civil status, the study reveals that the married IT managers have better level of implementation of IT security (2.98), while the single IT managers is 2.84. When the respondents are classified according to highest educational attainment, those who have master's degree have the highest weighted mean (3.00) of their level of prioritization of IT security compare to those with doctorate's degree ($\bar{x}$ = 2.76) and bachelor's degree ($\bar{x}$ = 2.92). Lastly, IT managers who are working

as fulltime have better weighted mean of level of prioritization of IT security (3.19) than the part-time IT managers with only $\bar{x}$ = 2.76.

3.3 The Relationship and Difference between the Prioritization and Implementation of IT Security in the Higher Education Institutions in the Philippines

The level of prioritization in all IT components presented in the study is rated high priority (Table 2). The result shows that these components are prioritized and need to be done in the next 3 years. On the other hand, all IT components presented in this study were rated moderately implemented (Table 3). The result shows that these components are already in the strategic plan but there is no action exercised. The level of prioritization on IT security has significant correlations at 0.01 level of confidence with the degree of implementation on IT security as shown in Table 4.

Table 4.
Test of Correlation between the Level of Prioritization and Degree of implementation of IT in the HEIs in the Philippines

IT Security	ρ-value	ρ -value (two-tailed test)	Remarks
	0.988 **	0.000	Significant

Legend: ** Correlation is significant at the 0.01 level (2-tailed)

Tables 5 shows that there is a significant difference between the level of prioritization and degree of implementation of IT security in the higher education institutions in the Philippines in terms of the total number of years of existence of the HEIs, total number of curricular offerings by the HEIs, annual IT expenditures of the HEIs, total Internet bandwidth of the HEIs, level of proficiency of the respondent's technical skills, rating of the respondents' human skills, rating of the respondent's conceptual skills, and extent of participation in decision-making of the respondents.

The mean values of all items in the IT security components show that the degree of implementation is less than the level of prioritization. It indicates that there is a disparity or significant difference in the implementation of IT security against the prioritization of IT security in the HEIs in the Philippines. This further implies that the HEIs in the Philippines have notable planning focusing on IT security; however, implementation plans are needed for improvement. This result may indicate also that IT managers in the HEIs in the Philippines do not fully implement formal strategizing and planning processes that meet established objectives and install disciplines to manage application acquisition and operation (Frenzel, 1999).

Table 5.
Test of Difference between the Level of Prioritization and Degree of Implementation of IT Security in the Higher Education Institutions in terms of the Respondents and HEI's Profile

IT Security Variables	F-value	ρ -value	t-value	ρ - value	Remarks
No. of years of existence of the HEI , Prioritization, Implementation	223.4951	3.24E-58	6.653031	3.26E-10	Significant
No. of curricular offerings of the HEI, Prioritization, Implementation	41.1359	6.36E-16	6.279007	3.58E-09	Significant
Annual IT Expenditures of the HEI, Prioritization, Implementation	8.819729	0.000209	5.491998	1.78E-07	Significant
Total Internet Bandwidth of the HEI, Prioritization, Implementation	11.68076	1.84877E-05	5.459868	3.16E-07	Significant
Respondent's Level of Proficiency of Technical Skills, Prioritization, Implementation	26.30184	3.66227E-11	6.602623	4.39E-10	Significant
Respondent's Rating of Human Skills , Prioritization, Implementation	94.73699	6.74346E-32	6.277503	2.96E-09	Significant
Respondent's Rating of Conceptual Skills, Prioritization, Implementation	82.41688	9.94233E-29	6.653031	3.26E-10	Significant
Respondent's Extent of Participation in Decision-making, Prioritization, Implementation	82.41688	9.94233E-29	6.653031	3.26E-10	Significant

Legend: t-values indicate the difference between prioritization and implementation of IT security

4. SUMMARY OF FINDINGS

The level of prioritization of IT security in the HEIs in the Philippines is described as high priority. This signifies that IT security components in the HEIs are prioritized and there is need to be done in the next 3 years. The degree of implementation of IT security has a description of moderately implemented. This implies that IT security is in the HEIs' strategic plan but there is no action that it has been done.

The level of prioritization of IT security has significant correlations at 0.01 level of confidence with the degree of implementation of IT security in the HEIs in the Philippines. The mean values of all items in the IT components show that the degree of implementation is less than the level of prioritization. It indicates that there is a disparity or significant difference in the implementation of IT security against the prioritization of IT security in the HEIs in the Philippines.

The result of this study is similar to the survey conducted of over 500 companies, cited by (O'Brien, 1999), adapted from Luftman (1997), on performance problems in managing information systems. The survey revealed that 16% of the respondents, highest in rank, showed that IT effort is poorly prioritized. In a separate survey, cited by (Chapman, 2004), on why CEOs fail, 70% of 10 CEOs who fail do so not because of bad strategy, but because of bad execution in the implementation. This may be a guide for the HEIs to properly and effectively implement IT security priorities to achieve organizational goals.

Likewise, the result of this study affirms the result of a survey conducted on why only one third of UK companies achieve strategic success 80% of MIS heads or directors said they had the right strategy and perhaps the right priorities but only 14% thought that they were implementing them well.

5. CONCLUSION AND RECOMMENDATION

The HEIs in the Philippines are working hard in terms of the management of IT security. Written privacy and security policies are the top priority in the HEIs in the Philippines but there is no enough extent of implementation. On the other hand, forensics in the HEIs in the Philippines is the least priority.

HEIs should strategically plan IT security and develop working methods of action for an effective implementation, administration and management of IT security. There must be campus awareness about IT security that will involve not only with the school administrators but as well as students, faculty staff, support units and services. HEIs should also be cautious on its priorities for the reason that implementation of IT security is expensive. HEIs may consider other alternatives and approaches that explain varied implementation issues. Turning plans into action-called phased approach (Chapman, 2004). HEIs may thoroughly identify performance factors with strategic initiatives and projects designed to develop and optimize departmental and individual activities in the institutions. HEIs in the Philippines should strategically establish an adequate protection to ensure confidentiality, integrity, and availability of the institution's resources.

Acknowledgements

I would like to extend my acknowledgement and appreciation to the following: 1) HEIs in the Philippines through their School Heads, IT Heads and Directors, for responding the request to answer the survey questionnaire; 2) Philippine Society of IT Educators, Computing Society of the Philippines, Philippine e-Learning Society, Cebu Educational Foundation for Information Technology, and the ICT Association in Dumaguete and Negros Oriental, for sharing their database of members; 3) Silliman University through the Faculty Development Committee, for funding the study on the analysis towards the IT landscape in the Philippines; 4) Advisers for their never-ending support.

Appendix

Map of the Philippines

Reference

Chapman, A. (2004). Strategy implementation and realization. Farsight Leadership Ltd. Retrieved on July 10, 2011from http://www.businessballs.com/businessstrategyimplementation.htm

Computerworld Philippines. (2010, January). Rising cybercrime rattles social networking world. *Computerworld Philippines*. Retrieved on December 5, 2011 from http://computerworld.com.ph/rising-cybercrime-rattles-social-networking-world/

Frenzel, C. W. (1999). Management of information technology, 3rd ed., Cambridge, MA: Course Technology Press.

Ingerman, B., Yang, C., and the 2010 EDUCAUSE Current Issues Committee. (2010) . Top-Ten IT Issues, 2010. EDUCAUSE. Retrieved on June 5, 2010 from http://www.educause.edu/EDUCAUSE+Review/EDUCAUSEReviewMagazineVolume45/TopTenITIssues2010/205503

O'Brien, J. (1999). Management information systems: Managing information technology in the Internetworked enterprise, 4th ed., Boston: MCGraw-Hill.

National Center for Education Statistics of the US Department of Education. http://nces.ed.gov/

Pfleeger, C. P. and Pfleeger, S. L. (2003). Security in Computing, 3rd ed., Pearson Education, Inc., New Jersey.

Philippines Business Guide. (2011). Helping your business grow internationally. UK Trade & Investment Philippines Markets Unit in collaboration with the British Posts in the Philippines, international trade teams and the Philippines-Britain Business Council: Crown. Retrieved on December 9, 2011 from http://www.ukti.gov.uk/download/108703_109035/Doing%20Business%20in%20the%20Philippines.pdf.html

Sembok, T. (2003). Ethics of information communication technology. UNESCO - Regional Unit for Social & Human Sciences in Asia and the Pacific. Retrieved on November 15, 2011 from http://www2.unescobkk.org/elib/publications/ethic_in_asia_pacific/239_325ETHICS.PDF

Sengupta, S. (2011, November). Phone hacking tied to terrorists. *The New York Times Company*. Retrieved on November 18, 2011 from http://www.nytimes.com/2011/11/27/world/asia/4-in-philippines-accused-of-hacking-us-phones-to-aid-terrorists.html?_r=1&ref=philippines

Shukla, A. (2010, January). Companies need more IT education to stop cyber crime. *MIS Asia*. Retrieved on November 20, 2011 from http://computerworld.com.ph/companies-need-more-it-education-to-stop-cyber-crime/

Tsang, S. (2007). Out of the ivory tower. *MIS Asia*. Special Issue. pp. 14-15.

Weaver, W. and Raulin, M. (2007). Random Number Generator Program. [Computer Software]. Graciano and Raulin Research Method Text Book. Retrieved on June 1, 2010 from http://www.mikeraulin.org/graziano7e/supplements/random_prog/randprog.htm