IJST EXPLORE International Journal of Science and Technology
CENTRE OF PROFESSIONAL RESEARCH PUBLICATIONS
ISSN 2049-7318

Journal of Science and Technology Volume 1 No. 7, July, 2012

Computer Security Awareness and Vulnerabilities: An Exploratory Study for Two Public Higher Institutions in Ghana

[1]Eldad Antwi-Bekoe, [2]Simon Gyasi Nimako

[1]Department of Information Technology Education, University of Education, Winneba. Ghana (UEW)

[2]Department of Management Studies Education, University of Education, Winneba, Ghana. (UEW)

ABSTRACT

The study is an exploratory study that evaluates computer security awareness and computer security vulnerabilities based on user practices among computer users in two public higher institutions in Ghana. Using a cross-sectional survey and a convenient sampling technique, the target population was identified as three subgroups namely faculty staff, administrative staff and students. The study reveals that different levels of computer security awareness exist among sub groups of each institution. Sub groups also differ in computer security vulnerabilities in some areas for each institution and between institutions. Key findings include differences in perception of remote connection to computer while on a network, seemingly inappropriate usage of anti-virus protection among computer users, computer security vulnerabilities created by the computer and password sharing behavior of users, among others. Limitations and future research have been suggested. The study also provides important managerial implications.

Keywords: *computer security awareness, vulnerabilities, Ghana, Higher institutions, security threats*

1. INTRODUCTION

With the ever-increasing use of information technology (IT), organizations around the globe are faced with the challenging task of protecting valuable resources from a never-ending onslaught of threats (Schweitzer, 2003). Throughout the developed world, governments, defense industries, and companies in finance, power, and telecommunications are increasingly targeted by overlapping surges of cyber attacks from criminals and nation-states seeking economic or military advantage (SANS Institute, 2009). This is consistent with the first joint Government and industry report into the extent and cost of cyber-crime across the UK in 2011 concludes that the cost of cybercrime is significant and growing (UK Cabinet Office & Detica, 2011). With society now almost entirely dependent on cyber space, this trend of growth in cybercrime and industrial espionage is likely to abound with prevailing attacks on financial institutions, corporate entities, individuals, government institutions, educational institutions and so on.

With a philosophy to supply knowledge to all who seek it, higher education institutions typically embraces an open environment. The networking environment is therefore faced with unique set of challenges that could present some dire consequences. Not only do these threats come from external world of spammers and hackers but also from within the campus environment originating from non academic computer using staff and some of the nation's brightest minds; professors, lecturers and students. With prevailing trend of identity theft and social engineering attacks, students' personal records stolen or in the hands of wrong individuals could as well have damaging consequences. Even more damaging to the individual could be the theft of proprietary knowledge assets before delivery. Unauthorized grade changes and persistent problems with registration or financial systems can undermine universities' viability. The likely cost of a major security breach extends even much further. For an institution, it connotes a public relations nightmare, real financial losses, far-reaching legal matters and for some countries, regulatory non-compliance penalties. To aggravate the situation, such a breach usually means a loss of confidence and trust in the institution, both internally and externally.

The gravity of the threats cannot be underestimated. To better appreciate the gravity of current computer security threats, and to develop effective strategies to tackle cyber crime requires a better understanding of its impact economically. For example, in December 2010, a reported security breach that involved records of over 76,000 students at the Ohio State University was estimated to cost the University $4 million in expenses related to investigative consulting, breach notification and credit card security. The other economic cost statistics from surveys by CSI-FBI (2005) and Ponemon institute (2011) involving a variety of US companies, as a result of security breaches are equally worrying. Such is the

severity of network-borne threats. Presumably, most reported figures are underestimated granted that most organizations fail to report security breaches they experience to law enforcement agencies. Firstly, for fear of negative media publicity and market reactions that could damage their market stock and or image. Secondly, for fear that competitors would use this negative publication to their advantage. Some organizations would also rather prefer to use civil remedy among other things.

In spite of this, it is still common to see very few Internet firewalls and rogue software - in terms of security - on the computers of the university's computer using community. This leaves the University network administrators a daunting task of fighting attacks. In Ghana, the evidence of the threat to organizations cannot be denied nor underestimated given the increased reliance on Information Technology. This sentiment is supported by the Internet Crime Complaint Center's annual Report that ranks Ghana as the sixth country among the top ten in the world where cyber crime is prevalent (IC3, 2009). Whereas progress has been made in terms of awareness, training and strategies to combat this menace in the developed countries, to the authors' knowledge, little progress has been made in Africa and for that matter Ghana.

Like any other Internet-facing security conscious organisation, the University of Education, Winneba (UEW) endorses a documented ICT policy framework for operational security practices for its ICT resources. The implementation of such policy is expected to translate into increasing user awareness of computer security issues. Computer security awareness (CSA) will serve to increase knowledge and offer improved chances of compliance to policy regulations and better computer security practices among users.

It is also important that management of policy guided institutions - like UEW and K-POLY - obtain a feedback on user awareness of computer security practices in order to develop strategies towards ensuring the effectiveness of the policy. Yet no empirical study has been conducted, as far as the researchers know, to evaluate user awareness of computer security practices and ICT Policy awareness on UEW-K network. Through personal observation of observable computer security practices among computer user communities of University of Education, Winneba (Kumasi Campus) and Kumasi Polytechnic, namely the academic staff, administrative staff and students, the authors found that users engage in practices that raise questions on CSA, ICT policy awareness and computer security vulnerabilities (CSV) among computer users on the University campus; and this has triggered this study.

The purpose of this study is to evaluate CSA and CSV based on user practices among UEW-K and K-POLY computer user communities. The study is also intended to increase awareness of computer security issues that threaten higher education in Ghana. The feedback of the study will enable ICT policy makers of UEW-K, K-POLY and other higher education institutions to improve upon their existing ICT policy. It will also inform stakeholders to enhance its policy implementation strategies.
Based on this the objectives of this study are outlined below:

a. To examine computer security awareness (CSA) and computer security vulnerabilities (CSV) at UEW-K and K-POLY.

b. To examine the differences in CSA and CSV among Faculty staff, Administrative staff and students within UEW-K and K-POLY.

c. To examine differences in CSV between computer users at UEW-K and K-POLY.

2. MATERIALS AND METHODS

2.1 Research Design, Population and Sampling

The study employed a cross-sectional survey which was appropriate for seeking the opinion of the target population about some phenomena, with a researcher designed questionnaire for data collection to answer the research questions (Cooper and Schindler, 2006).

The study sample consisted of students drawn from the Department of Information Technology Education (ITE) from UEW-K and the Department of Computer Science from K-POLY. Teaching and supporting staff were drawn from all (four) faculties at UEW-K, all (Six) faculties, two institutes and one centre at K-POLY; and administrative staff drawn from all the different faculties and administrative offices from both UEW-K and K-POLY. A total sample size of 720 respondents (comprising 370 from UEW-K and 350 from K-POLY respondents) was selected based on researchers' judgment because of cost and time constraints. A purposive sample of ITE students (from UEW-K) and computer Science students (from K-POLY) was chosen because the researcher believed they were more familiar with the concept of study and therefore most likely to provide more accurate responses. They were also more easily accessible to the researcher.

2.2 Data Collection Procedures

A self-administered, structured questionnaire was used to collect data from respondents as recommended for a large survey (Saunders et al 2000; Cooper and Schindler 2006; Malhotra and Birks, 2007). The questions sought

respondents' general computer usage practices and computer CSA. The questionnaire was pre-tested to a sample of 20 students selected by simple random method. This small size was guided by the suggestion by Fink (2003b in Saunders et al 2007) that the minimum of ten (10) members for pre-testing is adequate. Apart from an explanatory cover note that accompanied the questionnaire, each of them was told the purpose of the questionnaire and assured of anonymity and confidentiality of responses before they were given the questionnaire to respond to. Finally, after adjustments were made to get more effective instruments, the questionnaire was administered to the target population through personal contact by researchers. Again, respondents were first informed of the purpose, assured of anonymity and confidentiality of responses. They were then given the questionnaire to complete and were later retrieved from them at the shortest possible period agreed with them. This was between the periods of November 2, 2011 and December 18 2011. In order to get a more representative sample of the entire target population, the questionnaire was administered to Faculty Staff and Administrative Staff from all departments and administrative offices respectively. Fresh students, sophomores and juniors were the student respondents since they constituted the most active computer user student community on both campuses.

3. RESPONSE RATE

Out of the 370 questionnaires that were administered, 357 constituting 96.5% response rate was achieved. Out of this, there were 57 Faculty Staff, 69 of Administrative Staff and 231students. On the other hand, from 350 questionnaires were administered to K-POLY respondents, 313 constituting 89.4% response rate was achieved. Out of this, there were 106 Faculty Staff, 102 of Administrative Staff and 105 students. These numbers were adequate since a minimum sample of 30 is considered a large sample size for statistical analysis (Cooper and Schindler 2006, Saunders et al 2007).

4. DATA ANALYSIS

4.1 Perception of Computer Security Awareness (CSA)

Table 1 presents results of respondents' perception of CSA for UEW-K and K-POLY. It indicates that 84.3% and 84.7% for UEW-K and K-POLY respectively were aware that they could lose data as a result of malware infection while only 15.7% and 15.3% were not aware for UEW-K and K-Poly respectively. While 70.9% and 58.8% of respondents from UEW-K and K-Poly respectively were aware that remote connection to computer was possible when connected to a network, 29.1% and 41.2% respondents from UEW-K and K-Poly respectively were not aware. 73.4% and 67.7% from UEW-K and K-Poly respectively were aware of the benefits of having an Internet firewall, while 26.6% and 32.3% respectively were not aware.

4.2 Level of Computer Security Vulnerability (CSV)

Results on CSV have been presented in Tables 1 and 2. Table 1 presents results for CSV in areas such as online authentication practices, state of computer protection and personal security practices. Table 2 presents results on vulnerability from e-mail account practices and state of anti-virus/Internet security software. The following section describes the CSV from these two tables under three sub-headings: Online habits, State of computer protection and personal security practices.

Table 1: CSA and CSV between UEW-K and K-POLY

S/N	Item	UEW-K						K-POLY					
		Not sure		No		Yes		Not sure		No		Yes	
		No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
Perceptions													
1.	Perception of losing data…	26	7.3	30	8.4	301	84.3	22	7.0	26	8.3	265	84.7
2.	Remote connection to computer while...	46	12.9	58	16.2	253	70.9	65	20.8	64	20.4	184	58.8
3.	Awareness of the benefit(s) of …..	52	14.6	43	12.0	262	73.4	51	16.3	50	16	212	67.7
Account authentication habits													
4.	Browser stores my password	9	2.5	258	72.3	90	25.2	12	3.8	209	66.8	92	29.4

5.	Allowed someone to use my password before	17	4.8	265	74.2	75	21.0	13	4.2	234	74.8	66	21.1
6.	Shoulder surfing is OK.	21	5.9	244	68.3	92	25.8	14	4.5	202	64.5	97	31.0
State of computer protection													
7.	Antivirus software installed on computer	16	4.5	24	6.7	317	88.8	24	7.7	22	7.0	267	85.3
8.	Third party Internet firewall installed on computer	105	29.4	107	30.0	145	40.6	91	29.1	65	20.8	157	50.2
9.	Genuine operating system …	71	19.9	84	23.5	202	56.6	78	24.9	46	14.7	189	60.4
Personal security practices													
10.	Authentication is required …	6	1.7	76	21.3	275	77.0	10	3.2	90	28.8	213	68.1
11.	Backup of stored data occasionally done…	13	3.6	141	39.5	203	56.9	14	4.5	83	26.5	216	69.0
12.	One password for almost all accounts	9	2.5	189	52.9	159	44.5	11	3.5	171	54.6	131	41.9
13.	About eight or more character password(s) used	24	6.7	144	40.3	189	52.9	28	8.9	115	36.7	170	54.3
14.	Password(s) is a combination of alphabets and digits	15	4.2	145	40.6	197	55.2	19	6.1	150	47.9	144	46.0
15.	Password(s) is a combination of …	19	5.3	231	64.7	107	30.0	25	8	229	73.2	59	18
16.	File sharing enabled on computer	16	4.5	244	68.3	97	27.2	21	6.7	191	61.0	101	32.3
17.	Work computer is shared ….	19	5.3	270	75.6	68	19.0	24	7.7	212	67.7	77	24.6

4.2.1 Vulnerability from Online Habit

Online Account Authentication

From Table 1, for online account authentication habits, 25.2% and 29.4% of UEW-K and K-Poly respondents respectively responded that they allowed browsers to store their password(s) so that they don't have to type them again at subsequent logins, conversely 74.8% and 70.6% of UEWK and K-POLY respectively either responded that they did not allow browsers to store their password(s) or they were not sure whether they allowed browsers to store their password(s).

Regarding the use of password to log onto an online account, while 21.0% and 21.1% of UEW-K and K-Poly respondents respectively indicated that they had allowed someone to use their password to log onto their online account before, a greater percentage of 79.0% from both UEW-K and K-Poly either indicated that they had not allowed someone else to use their password to log on to their online account before or they were not sure if they had allowed someone before.

Regarding shoulder surfing, while 25.8% from UEW-K and 31.0% from K-Poly responded that they don't mind if a friend or colleague looked on as they keyed in their password, majority from UEW-K (74.2%) and K-Poly (69.0%) either indicated that they were mindful if a friend or colleague looked on as they keyed in their password or they were not sure if they were mindful.

Table 2 indicates the frequency with which respondents opened enticing e-mail (spam) and e-mail attachments. While 30.5% and 21.7% respondents from UEW-K and K-Poly respectively indicated that they never opened enticing e-mail messages from unknown persons, 49.8%

from UEW-K and 60.6% from K-Poly responded that they opened enticing e-mails always, often or rarely. 19.6% from UEW-K and % 17.6% from K-POLY indicated that that they were not sure as to how frequently they opened enticing e-mails.

For e-mail attachments, while 21.3% of UEW-K and 24.6% of K-Poly respondents indicated that they never opened enticing e-mail attachments, always or frequently, 63.1% from UEW-K and 65.9% from K-Poly responded that they opened enticing e-mails always, often or rarely. 15.7% from UEW-K and16.6% from K-POLY indicated that that they were not sure as to how frequently they opened enticing e-mails attachments.

4.2.2 Vulnerabilities from State of Computer Protection

Results on computer security vulnerability from the state of computer protection are presented in Table 1.

Types of Computer Protection

Regarding anti-virus installations, majority of UEW-K (88.8%) and K-Poly (85.0%) respondents were sure they had antivirus software installed on their computer(s), while only 11.2% and 15.0% of UEW-K and K-Poly respectively were either not sure or had no anti-virus software installed on their computer(s).

For third party Internet firewall installations on computer(s), considerable number from UEW-K (40.6%) and about half (49.8%) of K-poly respondents indicated that they had third party Internet firewall installed on their computer(s). On the other hand, a greater percentage of respondents from UEW-K (59.4%) either indicated that they had no third party firewall installed on their computer(s) or they were not sure if they had.

For genuineness of the operating system (OS) installed on computer(s), 56.6% and 60.4% of UEW-K and K-Poly respondents respectively responded that they had genuine OS installed on their computers, whereas 43.4% and 39.6% from UEW-K and K-Poly respectively either said they did not have a genuine OS installed or they were not sure if they had a genuine OS installed.

Personal Security Practices

Regarding personal security practices, while a greater percentage of UEW-K (77.0%) and K-poly (68.1%) respondents responded that they had user accounts that required authentication on boot-up of their computer(s), 23.0% and 32.0% of respondents from UEW-K and K-Poly respectively either indicated that their computer(s) required no authentication on boot-up or they were not sure if their computers required any authentication.

For the security of backing up important data on computer(s), 56.9% and 69.0% of UEW-K and K-Poly respondents respectively responded that they back-up important data on their computer(s) occasionally, while a considerable percentage of 43.1% from UEW-K and 31.0% from K-Poly either did not back-up important data or were not sure if they did.

Regarding the security of single password usage for multiple accounts, a considerable percentage of 44.5% and 41.9% from UEW-K and K-Poly respondents respectively responded that they use only one password for all their accounts that require password, while 52.9% and 54.6% of respondents from UEW-K and K-Poly respectively either indicate that they did not use one password for all their accounts or they were not sure if they used one password.

Regarding password length, about half of respondents from UEW-K (52.9%) and K-Poly (54.3%) indicated that their password(s) constitute eight characters or more. A considerable percentage of 47.1% and 45.7% from UEW-K and K-Poly respectively either indicated they use password(s) that did not constitute eight or more characters or were not sure if their password(s) constitute eight or more characters.

Regarding character combination for password, 55.2% and 46.0% respondents from UEW-K and K-Poly respectively indicated that they use hybrid password(s) of alphabets and digit(s), while 44.8% and 54.0% respectively responded that they either use otherwise or they were not sure. While 30.0% and 18% of UEW-K and K-Poly respondents respectively indicated that they use complex password(s) composed of alphabets, digits and symbols, a greater percentage from UEW-K (70.0%) and K-Poly (81.2%) either indicated that they use otherwise or they were not sure if their password is a combination of alphabets, digits and symbols. These reveal potential vulnerability that have been discussed under the discussion section.

For file sharing, while 27.2% of UEW-K respondents and 32.3% of K-poly respondents indicated they had enabled file sharing on their computers, a greater percentage from UEW-K (72.8%) and K-Poly (66.7%) either said they had not enabled file sharing on their computer(s) or they were not sure if they had enabled file sharing.

Regarding password sharing on work computer(s), 19.0% and 24.6% of UEW-K and K-Poly respondents indicated that they share their work computers with other colleagues and they share a common password for

authentication on this computer. However, most of the respondents from both UEW-K (80.9%) and K-Poly (75.4%) either indicated that they did not share a common password with colleague(s) for their work computer or they were not sure if they share password with colleagues.

4.3 Differences in Computer Security Awareness and Vulnerability

The study is intended to examine how computer awareness and vulnerability differs according to respondents' status with computer use in the two institutions – UEW-K and K-POLY. The results are summarized in Tables 3 and 4

Table 2: Computer Security Vulnerabilities (CSV): Online Habits

	Item	UEW-K										Differences among groups		
		Never		Rarely		Not Sure		Often		Always		Value	Df	p
	E-mail account practices	**No.**	**%**	**No.**	**%**	**No.**	**%**	**No.**	**%**	**No.**	**%**			
1.	Open Enticing messages	109	30.5	99	27.7	70	19.6	61	17.1	18	5.0			
2.	Open Enticing message attachments.	76	21.3	96	26.9	56	15.7	97	27.2	32	9.0			

		K-POLY									
		Never		Rarely		Not Sure		Often		Always	
	E-mail account practices	**No.**	**%**	**No.**	**%**	**No.**	**%**	**No.**	**%**	**No.**	**%**
1.	Open Enticing messages	68	21.7	100	31.9	55	17.6	69	22.0	21	6.7
2.	Open Enticing message attachments.	55	17.6	77	24.6	52	16.6	80	25.6	49	15.7

		UEW-K				K-POLY			
		FP		NFP		FP		NFP	
	Antivirus/Internet Sec. status	**No.**	**%**	**No.**	**%**	**No.**	**%**	**No.**	**%**
1.	Displayed message on antivirus/Intern. Security.	122	34.2	183	51.3	117	37.4	154	49.2

Frequency of Displayed message on antivirus/Intern. Security.

			UEW-K		K-POLY	
			FP	NFP	FP	NFP
1.	***Status of Anti-virus/ internet security***	Yes	115	174	110	132

	Test of differences				
	Kruskal-Wallis Test	Kruskal-Wallis ANOVA differences between UEW-K and K-Poly (opening spam vulnerability)	5.418	1	0.020
		Kruskal-Wallis ANOVA differences between UEW-K and K-Poly (opening attachment vulnerability)	4.202	1	0.040
		Kruskal-Wallis ANOVA differences between UEW-K and K-Poly (Status of anti-virus/internet security)	0.594	1	0.441
	T-test	T-test within UEW-K to determine differences in vulnerability for opening spam vulnerability	5.929	356	0.000
		T-test within UEW-K to determine differences in vulnerability for opening attachment vulnerability	10.973	356	0.000
		T-test within K-poly to determine differences in vulnerability for opening spam vulnerability	8.612	312	0.000
		T-test within K-Poly to determine differences in vulnerability for opening attachment vulnerability	12.682	312	0.000
		T-test within UEW-K to determine differences in vulnerability for opening spam vulnerability	14.236	304	0.000
		T-test within K-Poly to determine differences in vulnerability for opening attachment vulnerability	14.322	270	0.000

*p-value significant at 0.05; FP – Fully Protected, NFP – Not Fully Protected,

Differences According to Current Status

From Table 3, respondents from UEW-K differ in their perception of remote connection to computer while on the Internet/network (X^2 = 21.141, df = 2, p = 0.000) and awareness of the benefit of an Internet firewall (X^2 = 12.492, df = 2, p = 0.002). Specifically, students have highest awareness level (mean rank = 193.68) followed by faculty

Table 3: CSA and CSV According to Current Status - UEW-K

Item	Current status					
	X^2	Df	p	Student (MR)	Faculty (MR)	Adm (MR)
Perceptions						
1. Perception of losing data through virus infection/computer breakdown	5.365	2	.068	181.89	186.91	163.21
2. Perception of remote connection to computer while on internet/network	21.141	2	.000*	193.68	154.62	149.51
3. Awareness of the benefit(s) of an internet firewall	12.492	2	.002*	189.83	154.27	162.54
Account authentication habits						
4. Browser stores my password	9.966	2	.007*	171.24	177.61	205.81
5. Allowed someone to use my password before	9.729	2	.008*	169.69	190.85	200.53
6. Shoulder surfing is OK.	15.537	2	.000*	168.13	181.27	213.24
State of computer protection						
7. Antivirus software installed on computer	4.531	2	.104	181.03	186.16	166.65
8. Third party Internet firewall installed on computer	4.754	2	.093	171.03	188.80	197.73
9. Genuine operating system installed on computer	0.468	2	.791	181.41	175.74	173.59
Personal security practices						
10. Authentication is required to use my computer	2.508	2	.285	183.58	168.69	171.91
11. Backup of stored data occasionally done from computer	6.909	2	.032*	172.47	207.78	178.03
12. One password for almost all accounts	0.310	2	.856	180.68	178.45	173.86
13. About eight or more character password(s) used	2.679	2	.262	180.77	161.33	187.04
14. Password(s) used is a combination of alphabets and digits	0.201	2	.904	180.55	156.98	191.17
15. Password(s) used is a combination of alphabets, digits & symbols	5.027	2	.081	180.55	156.98	191.17
16. File sharing enabled on computer	3.630	2	.163	178.67	163.50	192.26
17. Work computer is shared and we use same password	20.150	2	.000*	171.71	163.10	215.65

*P-value significant at 0.05, MR – Mean Ranks, Adm – Administrative staff

TABLE 4: CSA and CSV According to Current Status - K-POLY

Item	Current status					
	X^2	Df	p	Student (M.R)	Faculty (M.R)	Adm (M.R)
Perceptions						
1. Perception of losing data through virus infection/computer breakdown	5.725	2	.057	146.84	165.24	158.90
2. Perception of remote connection to computer while on internet/network	10.561	2	.005*	175.20	139.47	156.48
3. Awareness of the benefit(s) of an internet firewall	2.431	2	.297	166.12	151.01	153.84
Account authentication habits						
4. Browser stores my password	4.759	2	.093	163.87	162.89	143.81
5. Allowed someone to use my password before	0.926	2	.629	152.08	161.02	157.89
6. Shoulder surfing is OK.	1.794	2	.408	159.09	162.62	149.01
State of computer protection						
7. Antivirus software installed on computer	9.453	2	.009*	143.39	163.60	164.16
8. Third party internet firewall installed on computer	9.159	2	.010*	155.32	140.83	175.53
9. Genuine operating system installed on computer	0.030	2	.985	156.15	158.00	156.83
Personal security practices						
10. Authentication is required to use my computer	1.018	2	.601	161.70	151.57	157.80
11. Backup of stored data occasionally done from computer	0.420	2	.811	153.31	159.51	158.19
12. One password for almost all accounts	1.031	2	.597	162.66	156.68	151.51
13. About eight or more character password(s) used	0.539	2	.764	160.46	152.54	158.08
14. Password(s) used is a combination of alphabets and digits	5.507	2	.064	160.15	167.98	142.34
15. Password(s) used is a combination of alphabets, digits & symbols	1.028	2	.598	153.24	155.26	162.66
16. File sharing enabled on computer	8.143	2	.017*	173.20	142.81	155.07

17. Work computer is shared and we use same password	7.798	**2**	.020*	140.69	163.09	167.46

*P-value significant at 0.05, MR – Mean Ranks, Adm – Administrative staff

staff (mean rank = 154.62) and administrative staff (mean rank = 149.51) with respect to remote connection to computer while on the Internet/network. Again, students seem to have highest awareness of the benefits of an Internet firewall (mean rank = 189.83) followed by administrative staff (mean rank = 162.54) and faculty staff (mean = 154.27).

Again, from Table 3, respondents also differ in the practice of allowing browsers to store their passwords when online ($X^2 = 9.966$, df = 2, p = 0.007). Specifically, administrative staff is the subgroup mostly engaged in this practice (mean rank = 205.81) followed by faculty staff (mean rank = 177.61) and students (mean rank = 171.24) with respect to the practice of allowing browsers to store their password. Administrative staff are therefore the most vulnerable sub group followed by faculty staff and then students with respect to threats that exploit password files of browsers.

Likewise respondents differ in the behavior of having allowed someone else to use their credentials to log onto their online account before ($X^2 = 9.729$, df = 2, p = 0.008). Specifically, administrative staff were mostly engaged in this practice (mean rank = 200.53), followed by faculty staff (mean rank = 190.85) and students (mean rank = 169.69). Administrative staff appear to be the most vulnerable followed by faculty staff and students with respect to third party intrusions and other security threats that exploit this behavior.

Moreover, respondents differ in their attitude to an on-looking 'trusted' friend/colleague when keying in their password on their computer(s) ($X^2 = 15.537$, df = 2, p = 0.000). Specifically, administrative staff appear to show the least concern (mean rank = 213.24) followed by faculty staff (mean rank = 181.27) and students (mean rank = 168.13) with respect to shoulder surfing by 'trusted' friend/colleague. This implies that administrative staffs of UEW-K are the most vulnerable followed by faculty staff and students with respect to social engineering attacks (and other threats) that exploit behaviors such as trust.

For personal security practices, respondents differ in their efforts of making occasional backups for important data ($X^2 = 6.909$, df = 2, p = .032) and the practice of sharing computer(s) including the password for its use ($X^2 = 20.150$, df = 2, p = .000). Specifically, faculty staff of UEW-K appear to make the most effort in occasionally backing up their important data (mean rank = 207.78) followed by administrative staff (mean rank = 178.03) and students (mean rank = 172.47). Administrative staff seem to rank highest (mean rank = 215.65) followed by students (mean rank = 171.71) and faculty staff (mean rank = 163.10) with respect to the practice of sharing work computer(s) and the password for its use. Students of UEW-K appear to be the most vulnerable followed by administrative staff and faculty staff with respect to security threats that result in data loss. Such threats may include accidental deletion, system failure, corruption of data, etc. Conversely, Administrative staff seem the most vulnerable sub group followed by students and faculty staff with respect to security threats emerging from sharing work computer (including the password for its use).

From table 4, respondents from K-POLY differ in their perception of remote connection to computer while on the Internet/network ($X^2 = 10.561$, df = 2, p = .005). Specifically, students appear to have the highest level of awareness (mean rank = 175.20) followed by administrative staff (mean rank = 156.48) and faculty staff (mean rank = 139.47).

Regarding the state of computer protection, respondents differ in the installation of antivirus software on computer(s) they use ($X^2 = 9.453$, df = 2, p = .009) and the installation of third party firewalls ($X^2 = 9.159$, df = 2, p = .010). Specifically, administrative staff seem to have the highest deployment of anti-virus software technology (mean rank = 164.16) followed by faculty staff (mean rank = 163.60) and students (mean rank= 163.47). Again, administrative staff seem to have the highest deployments (mean rank = 175.53) followed by students (mean rank = 155.32) and faculty staff (mean rank = 140.83) with respect to third party firewall deployments. This implies that while students appear to be the most vulnerable in terms of malware attacks, faculty staff seems to be the most vulnerable in terms of threats associated with unprotected systems (third party firewall protection). Administrative staff appears to be the least vulnerable in terms of deployments for both antivirus and third party firewall technologies.

For personal security practices, respondents differ in the practice of enabling file sharing on computer(s) they use ($X^2 = 8.143$, df = 2, p = .017) and the practice of sharing computer(s) including the password for its use ($X^2 = 7.798$, df = 2, p = .020). Specifically, students were mostly engaged in the practice of enabling file sharing on the computers they use (mean rank = 173.20), followed by administrative staff (mean rank = 155.07) and faculty staff (mean rank = 142.81). Administrative staff appear to

be the subgroup with the most significant involvement in the practice of sharing work computer and the password for its use (mean rank = 167.46) followed by faculty staff (mean rank = 163.09) and students (mean rank = 140.69). Students therefore appear to be the most vulnerable to security threats associated with the misuse of file sharing functionality followed by administrative staffs and faculty staffs. On the other hand, administrative staff seems to be the most vulnerable followed by faculty staff and students with respect to security threats associated with the sharing of work computer and password to access its resources.

Differences in Vulnerability According to Institution

Table 5 shows a summary of how respondents from UEW-K and K-POLY differ on CSA and CSV.

Respondents differ in the deployments of third party Internet firewall (X^2 = 8.511, df = 1, p = .004) as the mode of protection against unauthorized access to computers. Specifically, computer users at K-POLY appear to have a higher deployment of third party firewall technologies on computers (mean rank = 357.19) compared to users at UEW-K (mean rank = 316.49). This could imply that UEW-K computer users are more vulnerable compared to K-POLY with respect to unauthorized access to the computers they use. This is particularly true if computer users at UEW-K do not have any system firewall (OS firewall) enabled on the OS they use.

Respondents differ in their personal security practices in the areas of access control to computer use (X^2 = 6.440, df = 1, p = .011), efforts in making occasional backups of important data (X^2 = 11.665, df = 1, p = .001), the practice of using hybrid character passwords (X^2 = 4.858, df = 1, p = .028), the practice of using complex character passwords (X^2 = 7.331, df = 1, p = .007) and the practice of sharing computer(s) including the password for its use (X^2 = 4.858, df = 1, p = .028). Specifically, significantly higher proportion of UEW-K computer users seem to employ password access control mechanism on their computers (mean rank = 349.25) compared to K-POLY (mean rank = 319.82). Again, UEW-K seem to have significantly more computer users employing hybrid character password(s) authentication (mean rank = 349.15) compared to K-POLY (mean rank = 319.93). Likewise UEW-K appear to have significantly more users employing complex character password authentication as their access control mechanism on computer(s) they use (mean rank = 350.91), compared to K-POLY (mean rank = 317.92). Conversely, K-POLY seem to have a higher number of computer users employing occasional backups of their important data (mean rank = 358.61) compared to UEW-K users (mean rank = 315.24). Computer users at K-POLY appear to also have

TABLE 5: Differences in CSA and CSV BETWEEN UEW-K AND K-POLY

Item	Awareness and Vulnerability				
	X^2	Df	p	UEW-K (M.R)	K-POLY (M.R)
Perceptions					
1. Perception of losing data through virus infection/computer breakdown	0.017	1	.897	334.93	336.15
2. Perception of remote connection to computer while on internet/network	11.536	1	.001*	355.57	312.61
3. Awareness of the benefit(s) of an internet firewall	2.189	1	.139	343.78	326.05
Account authentication habits					
4. Browser stores my password	2.164	1	.141	327.25	344.91
5. Allowed someone to use my password before	0.014	1	.907	336.12	334.17
6. Shoulder surfing is OK.	1.470	1	.225	328.49	343.50
State of computer protection					
7. Antivirus software installed on computer	1.605	1	.205	340.65	329.62
8. Third party internet firewall installed on computer	8.511	1	.004*	316.49	357.19
9. Genuine operating system installed on computer	2.900	1	.089	324.95	347.53
Personal security practices					

10. Authentication is required to use my computer	6.440	1	.011*	349.25	319.82
11. Backup of stored data occasionally done from computer	11.665	1	.001*	315.24	358.61
12. One password for almost all accounts	0.317	1	.573	338.95	331.57
13. About eight or more character password(s) used	0.400	1	.527	331.57	339.98
14. Password(s) used is a combination of alphabets and digits	4.858	1	.028*	349.15	319.93
15. Password(s) used is a combination of alphabets, digits & symbols	7.331	1	.007*	350.91	317.92
16. File sharing enabled on computer	3.444	1	.063	324.63	347.90
17. Work computer is shared and we use same password	4.858	1	.028*	323.38	349.33

*P-value significant at 0.05, MR – Mean Ranks

significantly more computer users (mean rank = 349.33) than UEW-K (mean rank = 323.38) with respect to the practice of sharing work computer(s) and the password for its use.

This implies that K-POLY computer users are more vulnerable than UEW-K computer users with respect to threats that exploit easy access to unprotected computers (in terms of access control). Such threats may include access to confidential data, privileges, installation of key loggers via external USB drives, etc. by unsuspecting miscreants if computer is left unattended. Likewise, computer users at K-POLY seem more vulnerable to hybrid mode password cracking attacks and brute force attacks by crackers. Again, computer users at K-POLY seem to be more vulnerable compared to UEW-K users with respect to security threats associated with sharing of work computer resources and the password for its access. Such threats may include difficulty to determine policy violators from audit logs, perpetrators of compromises, etc. On the other hand, computer users at UEW-K appear to be more vulnerable to the risks associated with data loss, accidental deletion or corruption of important data compared to K-POLY computer users. This may be because computer users at K-POLY must have experienced relatively more compromises than UEW-K computer users making them more conscious of data recovery methods to salvage their important data.

5. DISCUSSION AND IMPLICATION

Researchers would want to devote much attention to the areas of computer security that users appear to be more vulnerable.

Based on the data analysis, the study found that the respondents appear to be less vulnerable for the following areas: threats from stored password in user browsers, third party intrusions through sharing of password with others, third party intrusions through shoulder surfing, malware attacks, pirated OS, poor (or no) access control mechanisms implementations on computers from boot up, back-up of important data, enabling file sharing, and sharing computer resources including the password for its use.

To begin with, this study found that most of the respondents from both institutions appear to be less vulnerable to malware attacks. Even though majority of UEW-K (88.8%) and K-Poly (85.0%) respondents had installed antivirus software on their computer(s), table 2 indicates that about half of both UEW-K (51.3%) and K-poly (49.2%) respondents indicated that the most frequently displayed status of their Internet security or antivirus software was 'Your subscription has expired', 'You are not fully protected' or 'Your antivirus program is out of date'.

Anti-virus software continues to top the list of technologies deployed to fight malware (CSI survey, 2010). It is likely that the awareness and deployment of anti-virus software protection are high among higher education respondents as indicated by UEW-K and K-Poly respondents. However, a feedback on whether the installed anti-virus softwares were genuine and had valid subscriptions was not pursued in this study. The few who had no antivirus or were not sure are most likely vulnerable to malware attacks. CSI survey (2010) report maintains that malware incidents continue to be the most frequently occurring attack among organizations. This could imply major security vulnerability among respondents where these anti-virus installations have expired subscriptions. This is confirmed by the results from the cross tabulation (Table 2) indicating that most respondents who have anti-virus installed on their computers have their anti-virus expired/out of date. An out of date virus scanner is only marginally better than no virus scanner at all (Microsoft TechNet, n.d.). A secondary implication is that the networks of the organizations used by these respondents are likely to be vulnerable as the computers used by these respondents become the weak link in the chain of security within the network.

The implication of this finding is that there is the need for management of these two institutions to increase CSV education to enlighten computer users on computer security measures to ensure that their computer systems are fully protected through continuous anti-virus/internet security updates and avoiding rogue or pirated anti-virus/internet security software since their failure rate could be high.

Again, the study found that about half of respondents appear to be vulnerable to unauthorized access (via penetration attacks) to their computer systems. CSI Survey report (2010) maintains a high level (94.9%) of firewall deployments among respondents on networks. This is likely to be an indication of high level of awareness, conscious effort to protect systems and compliance to policies. This is not reflective in this study. This could possibly be due to increased reliance on operating system (OS) firewall. On the other hand, it could also be low awareness level among respondents regarding the benefits of third party firewall installations. Even though third party firewalls do not offer perfect protection against threats on the Internet or network, most of them offer egress filtering in addition to ingress filtering as opposed to the solely ingress filtering offered by the default behavior of most system (OS) firewalls. Threats initiated by some malware from services running on computers may therefore leave an element of vulnerability among most system firewall users. It is therefore necessary to monitor and filter egress traffic.

The implication of this finding is that there is the need for management of these two institutions to increase CSA and CSV education to enlighten computer users on computer security measures to ensure that their computer systems are fully protected through installation and effective use of third-party firewall firewall or proper configuration of OS firewalls.

The study also revealed that a considerable number of UEW-K and K-POLY respondents appear to be vulnerable to a possible compromise of all their accounts if their password is cracked by an attacker. Florencio and Herley (2007) found that an average web user has about 25 accounts that require password. If users use the same password at multiple sites, it could be very dangerous because if a password is cracked at one site, the attacker is likely to be able to impersonate the user at other sites (Panko, 2009). Other servers on which such users authenticate themselves could therefore be compromised through unauthorized access. This implies that about 40% of the respondents from both UEW-K and K-POLY are likely to be vulnerable to such incidents on the networks which they connect.

Users should be educated in the use of multiple passwords for multiple online or computer system accounts. This is because of the common notion that it is more likely to have multiple accounts that uses the same logon password to be compromised by an attacker than it will be for the same set of multiple accounts if it is authenticated by different passwords.

A finding worth of note is that a considerable number of respondents from both UEW-K and K-POLY appear to be vulnerable to different forms of password cracking attacks. Even though combining letter cases, digits and punctuation symbols is recommended for passwords, increasing the password length (number of characters in the password) in such combinations is known to increase the time needed for a brute force attack to succeed by a factor of 70 (Panko, 2010). Passwords should be at least eight characters long and even longer passwords are desirable (Panko, 2010). This implies that about half of the respondent from both institutions may have passwords strong enough to withstand attack complexities less than brute force. This may be due to high level of awareness and consciousness among computer users or possibly a forced compliance to eight character password policy from servers on which they authenticate themselves. The rest that indicated less than eight character password usage may likely be vulnerable to weaker forms of password cracking attacks.

It is therefore recommended that users use password with multiple characters made up of combination of alpha numeric and symbols up to a minimum of eight characters.

Moreover, it is found that about 55.2% and 46.0% or more respondents from UEW-K and K-Poly respectively used password(s) that may likely be vulnerable to different forms of hybrid mode attacks while about 30.0% and 18% from UEW-K and K-Poly respectively used password(s) that could only be compromised by brute force attacks. The main problem with passwords is that most users pick very weak passwords (Panko, 2010). Florencio and Herley (2007) found that users choose passwords with an average bitstrength 40.54 bits. Hybrid word or name passwords are cracked almost as quickly as passwords made of simple words and names (Panko, 2010). Even though hybrid passwords seem better than common name or word passwords, 55.2% and 46.0% respondents from UEW-K and K-Poly respectively are likely to be vulnerable to hybrid mode attacks on compromised servers and client PCs. The minority few from UEW-K and K-POLY who use complex passwords may unlikely be compromised only by brute force attacks. The probably vulnerable majority may likely be due to low level of awareness or user apathy among users.

5.1 Differences in computer security vulnerability

Differences according to current status

Based on the data analysis, the study found that differences exist among respondents from UEW-K in their vulnerability to computer security threats according to current status in the following ways:

- Administrative staff are significantly most vulnerable, followed by faculty staff and students with respect to the practice of allowing browsers to store their password(s). This level of vulnerability probably exists from a misconceived notion that passwords are no longer personal. Being the subgroup with significantly the highest practice with respect to sharing work computer and the password for the computer's use (table 3), they must have acquired this misconceived notion. On the other hand it could also be low level of awareness about security risks posed or a combination of the both. Hubbard (2002), warns that "The less 'security awareness' is present in an organization, the greater the vulnerability is with respect to that organization's people, because if they do not know how to act in a secure manner, they won't". Students are the least vulnerable probably because they have acquired some computer security consciousness by virtue of their subject area experience.

- Administrative staff were most vulnerable, followed by faculty staff and students with respect to the practice of having allowed somebody else to use their password to log onto their online accounts. Again, this vulnerability is probably routed in an acquired misconceived notion that passwords are no longer personal. This may be inferred from the outcome that admin staff happened to be the subgroup with significantly the highest practice of sharing work computer and the password for the computer's use. The tendency for faculty staff to delegate tasks to secretaries and other data entry clerks to work on their work/personal PC(s) must have contributed to being the second highest vulnerable sub group.

- Again, Administrative staff of UEW-K are the most vulnerable followed by faculty staff and students with respect to social engineering attacks (and other threats) that exploit behaviors such as trust. This is probably because Administrative staff must have lost the value of secrecy regarding password. Being the subgroup with significantly the highest practice with respect to sharing work computer and the password for the computer's use, must have contributed to this lost value. Majority of their colleagues and some co-workers may therefore be considered trusted. Students are the least vulnerable probably because they have acquired some CSA values and consciousness by virtue of their subject area experience.

- UEW-K students appear to be the most vulnerable followed by administrative staff and faculty staff with respect to security risks of losing important data in the event of a 'disaster'. This could probably be because students attach relatively less importance to the kind of data that they hold on their computers. Relatively more important data may be administrative documents used by administrative staff. The least vulnerable position of faculty staff could probably be the already known notion that all faculty staff hold and work on relatively the most sensitive (or important) data such as students academic records, examination materials, intellectual property etc. Budman (2011) also found that the tendency to backup correspond with income, level of education and employment. This must have influenced this pattern of vulnerability.

Administrative staff seem the most vulnerable sub group followed by students and faculty staff with respect to security threats emerging from sharing work computer (including the password for its use). The high vulnerability among admin staff could most likely be as a result of the situation of a low computer to administrative staff ratio compelling the sharing behavior. Preference for, and the convenience of sharing the same account on shared computer(s) rather than switching in between user accounts and employing different password(s) could be a contribution to the high vulnerability among admin staff. Low awareness levels among admin staff and management regarding the security risks involved may have also accounted for this practice, leading to high vulnerability. Faculty staff are least vulnerable possibly because the data they work on or hold on their computers are deemed relatively most sensitive and requires an element of privacy.

For K-POLY, students appear to be the most vulnerable followed by faculty staff and admin staff with respect to malware attacks. Even though there seem to be a high installation of anti-virus software (85.3%) among respondents of K-POLY, it is possible that majority of these deployments are accounted for by faculty and admin staff. Administrative staff are least vulnerable probably because of their high awareness level and relatively extensive deployment of Internet security software for office computers used by the administrative staff.

Faculty staff seems to be the most vulnerable in terms of threats associated with unprotected systems (third party firewall protection) followed by students and admin staff. The significantly high level of vulnerability among faculty staff is most likely due to low awareness regarding the possibility of remote connection to computer while on a network (table 4).

Administrative staff appears to be the least vulnerable in terms of deployments for both antivirus and third party firewall technologies probably because of their high awareness level and relatively extensive deployment of Internet security software for office computers used by the administrative staff.

Students appear to be the most vulnerable to security threats associated with the possible misuse of file sharing functionality followed by administrative staff and faculty staff. This is probably because students are almost twice as likely to share files including pictures, music videos etc. as non-students (Johnson, n.d). This is consistent with the finding that College students lead other Internet users in file sharing of all kinds (Jones et al, 2002).

Administrative staff seems to be the most vulnerable followed by faculty staff and students with respect to security threats associated with the sharing of work computer and password for its use. The high vulnerability among admin staff could most likely be as a result of the situation of a low computer to administrative staff ratio compelling the sharing behavior. Preference for, and the convenience of sharing the same account on shared computer(s) rather than switching in between user accounts and employing different password(s) could be a contribution to the high vulnerability among admin staff. Low level of awareness among admin staff and management regarding the security risks involved may have also accounted for this practice, leading to high vulnerability.

Differences in Vulnerability According to Institution

- Computer users at UEW-K have a higher vulnerability compared to K-POLY with respect to unauthorized access to the computers they use. This is particularly true if computer users at UEW-K do not have any system firewall (OS firewall) enabled on the OS they use.

- Significant number of computer users at K-POLY are more vulnerable than computer users at UEW-K with respect to third party intrusions (and other threats) that exploit computers systems with no access control mechanisms on start up.

- Computer users at UEW-K are more vulnerable than computer users at K-POLY with respect to loosing important data in the event of a disaster.

- Computer users at K-POLY seem to be significantly more vulnerable than computer users at UEW-K with respect to hybrid mode password cracking attacks.

- Likewise computer users at K-POLY appear to be significantly more vulnerable than users at UEW-K with respect to brute force password cracking attacks.

- Computer users at K-POLY are more vulnerable than UEW-K users with respect to security threats that exploit practices such as computer resource and password sharing.

- This implies that K-POLY computer users are more vulnerable than UEW-K computer users with respect to threats that exploit easy access to unprotected computers (in terms of access control). Such threats may include easy access to confidential data, privileges, installation of key loggers via external USB drives, etc. by unsuspecting miscreants if computer is left unattended. Likewise, computer users at K-POLY seem more vulnerable to hybrid mode password cracking attacks and brute force attacks by crackers. Again, computer users at K-POLY seem to be more vulnerable than UEW-K users with respect to security threats associated with sharing of work computer resources and the password for its access. Such threats may include difficulty to determine policy violators from audit logs, perpetrators of security breaches from within the network, etc. On the other hand, computer users at UEW-K appear to be more vulnerable to the risks associated with data loss, accidental deletion or corruption of important data compared to K-POLY computer users. This may be because computer users at K-POLY more frequently experience relatively more compromises than UEW-K computer users. This makes them more conscious of data recovery methods to salvage their important data.

General Guidelines to Reduce CSV

Apart from the above implications and recommendations discussed, the following are other general strategies for managing CSA and CSV in both institutions:

- The implication of this finding is that there is the need for managmenet of these two institutions to increase CSA education to enlighten computer users on computer security measures for managing

password stored in browsers. Users could avoid sharing their computers systems with other untrusted users, de-active the password storage feature of browsers after use, or users could avoid the practice of enabling password storing feature in browsers in some cases.

- Computer users should not share password at all, unless with untrusted persons.
- Computer users should be alert and ensure there are no on-lookers when keying their password in their computer systems.
- Computer users should always use genuine OS
- Computer users are to ensure that anti-virus programs installed on their computer systems have valid subscriptions and are updated regularly.
- Computer users should encourage third party firewall deployments on computer systems or be sure systems firewall is enabled and configured correctly on computer systems
- Computer users should ensure authentication as an access control measure for use of computer systems.
- Users should have back-ups of all important data on computer systems occasionally.
- Computer users should not enable file sharing, enable file share with trusted users
- Even if computer use is shared, there should be separate accounts for the users.

5.2 Limitations and Future Research

CSV in this study was explored from the perspective that CSV is anything that offers a potential avenue of attack against a computer system or network and not as a security exposure that results from a product flaw, and which the maker of the product need to fix (TechNet, 2012). Even though this study provides a foundational insight into CSA and CSV levels within higher educational institutions (UEW-K and K-POLY), I.T. education is relatively new within both institutions. Interpreting and understanding questionnaire items (and therefore responses) from non-I.T. biased respondents may have influenced the findings. This study also employed a convenient sampling technique which could have possibly influenced the outcome of the study. An improved sampling technique could be adopted in future studies. Again, student responses might have been influenced by their subject area experience and therefore may not entirely reflect responses from the entire student population. Moreover, a more quantitative and robust approach could be adopted in future studies. Future research could examine the factors that decide users' computer security vulnerability.

6. CONCLUSION

CSV exist among computer users within higher educational set ups and differ in many potential avenues according to status. The CSV also differ from institution to institution even though similarities may exist. The right technologies will need to be deployed and configured correctly to minimize CSV. CSA training programs are therefore needed within higher educational set ups irrespective of the level of vulnerability among computer users, guided by the tenet that an organization's overall security is only as strong as its weakest link. Awareness alone will not be enough given that user apathy and deliberate defiance exist and needs to be battled. Strategies to enforce compliance to organizational policies need to be considered and policy implementations need to be evaluated on an ongoing basis to ascertain its effectiveness.

REFERENCES

[1] Panko, R.R. (2009). Business data networks and telecommunications. 7 th Edn., Prentice Hall, USA.

[2] Ponemon Institute. (2011). Second annual cost of cyber crime study. Research Report, Traverse City, Michigan, MI. Retrieved from: http://www.arcsight.com/collateral/whitepapers/2011_Cost_of_Cyber_Crime_Study_August.pdf

[3] Computer Security Institute, (2011). 2010/2011 CSI Computer Crime and Security Survey. 6 June 2011. Retrieved from: http://www.gocsi.com/survey

[4] Puhakainen, P. (2006). A design theory for information security awareness, Academic Dissertation, Faculty of Science, University of Oulu, Finland. ISBN: ISBN 951-42-8114-4. Retreived from:http://herkules.oulu.fi/isbn9514281144/isbn9514281144.pdf.

[5] Enterasys Security Networks. (2009). Securing the university network. Retreived from: http://www.enterasys.com/company/literature/dscc_brochure-wp.pdf.

[6] Karolewski, A. M., Coon A., Raffensperger S., Ometere, E.L. (2005). Home computer security awareness. Research Project, Indiana University of

Pennsylvania, IN. Retrieved from: http://www.cosc.iup.edu/www/studentResearch/womenofcs_files/docs/pacise_paper.pdf.

[7] Detica. (2011). The cost of cyber crime. A detica report in partnership with the office of cyber Security and information assurance in the cabinet office, 2011. Detica Limited, UK. England, Surrey Research Park. 02.11.DET.CCR.001.

[8] D'Amico, D. A. (2002). What does a computer security breach really cost? Global information assurance certification paper. SANS Institute. Retrieved from: http://www.avatier.com/files/pdfs/CostsOfBreaches-SANSInstitute.pdf.

[9] Fowler, R.T. (2007). Making security awareness efforts work for you. Retrieved from: http://www.sans.org/reading_room/whitepapers/awareness/making-security-awareness-efforts-work_32763.

[10] Nellis, R. (2003). Creating an I.T. security awareness program for senior management. Retrieved from: http://www.sans.org/reading_room/whitepapers/policyissues/creating-security-awareness-program-senior-management_992.

[11] Internet Crime Complaint Centre. (2010). 2009 Internet crime report. Retrieved from: http://www.ic3.gov/media/annualreport/2009_IC3Report.pdf.

[12] Hubbard, W. (2002). Methods and techniques of implementing a security awareness program. Retrieved from: http://www.sans.org/reading_room/whitepapers/awareness/methods-techniques-implementing-security-awareness-program_417.

[13] Messmer, E. (2008). Cyber espionage seen as growing threat to business, government. Network World. Retrieved from: http://www.networkworld.com/news/2008/011708-cyberespionage.html #disqus_thread.

[14] Tetterington, G. (2011). Enterprises not taking threat of cyber espionage seriously, Ovum finds. Retrieved from: http://ovum.com/press_releases/enterprises-not-taking-threat-of-cyber-espionage-seriously-ovum-finds/.

[15] Wilson, M. and Hash, J. (2003). Building an Information Technology Security Awareness and Training Program. National Institute of standards and Technology (NIST) Special Publication 800-50.

[16] Wilson, M and Hash, J. (2003). Building an information technology security awareness and training Program. National Institute of standards and Technology (NIST) Special Publication 800-50. Retrieved from: http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf.

[17] Microsoft TechNet (2012). 10 immutable Laws of Security. Retreived from: http://technet.microsoft.com/en-us/library/cc722487.aspx

[18] Hoffman, C. (2012). Windows 7 Firewall: How It Compares Against Other Firewalls. Retrieved from: http://www.makeuseof.com/tag/windows-7-firewall-compares-firewalls/

[19] Boateng, R., Longe, O., Mbarika, V., Avevor, I., Isabalija, S. R., (2010). Cyber crime and criminality in Ghana: Its forms and implications. Proceedings of the Sixteenth Americas Conference on Information Systems (AMCIS), Lima, Peru, August 12-15, 2010.

[20] KGBS, (2009). About backup habits, risk factors, worries and data loss of home PCs. Retrieved from: http://www.kabooza.com/globalsurvey.html

[21] Meyer, R. (2007). Secure authentication on the Internet. Retrieved from: http://www.sans.org/reading_room/whitepapers/securecode/secure-authentication-internet_2084

[22] Kabooza Global Backup Survey (2009). About backup habits, risk factors, worries and data loss of home pcs. Retrieved from: http://www.kabooza.com/globalsurvey.html

[23] Johnson, M.E., McGuire, D. and Willey, M.D. (n.d.) Why file sharing networks are dangerous. Center for Digital Strategies, Tuck School of Business, Dartmouth College, Hanover NH 03755 *Communications of the ACM*

[24] Jones, S., Clarke, M. L., Cornish, S., Gonzales, M., Johnson, C. Lawson, N.J., Smith, S., Bickerton, H.S., Hansen, M., Lengauer, G., Oliveria, L., Prindle, W., Pyfer, J. (2002). The Internet Goes to College: How students are living in the future with today's technology. Pew Internet & American Life Project. Washington, D.C.

[25] Budman, G. (2011). 94% of computer users still risk data loss. Retrieved from: http://blog.backblaze.com/2011/07/12/94-of-computer-users-still-risk-data-loss/

[26] Schweitzer, D. (2003). How to toughen the weakest link in the security chain. Retrieved from: http://www.computerworld.com/s/article/77360/How_to_toughen_the_weakest_link_in_the_security_chain_

[27] Schweitzer, D. (2003). Incident Response: Computer forensics toolkit. USA: Wiley Publishing, Inc.

[28] Cooper, D.R. and Schindler, P. S. (2006). Business Research Methods (9th ed.), empirical investigation", Journal of Service Research, 1 (2), pp. 108-28.

[29] Gouda, M.G., Liu, A.X., Leung, L.M. and Alam, M.A. (n.d). Single password, multiple accounts. Department of Computer Science. University of Texas at Austin. Retrieved from: http://www.cse.msu.edu/~alexliu/publications/Password/password.pdf

[30] Malhotra, N. K. and Birks, D. F. (2007), Marketing Research, An applied Approach (3rd Ed.) USA: Prentice Hall, Inc.

[31] Britt, P. (2005). Protecting against data breaches in higher education. *Information Today;* Jul/Aug 2005; 22, 7; ABI/INFORM Research. pp.1

[32] Florencio, D. and Herley, C. (2007). A largescale study of web password habits. Proceedings of International World Wide Web Conference 2007, May 8-12, 2007, Banff, Alberta, Canada. ACM 978-1-59593-654-7/07/0005.

[33] Verizon. (2010). 2010 Data breach investigations report. USA: Verizon RISK Team in cooperation with the USSS.

[34] JMU(2012). Microsoft windows file sharing risks. Retrieved from: www.jmu.edu/computing/security/info/msfileshar.shtml#1. James Madison University Harrisonburg, VA.

[35] TechNet (2012). Definition of a security vulnerability. Retrieved from: http://technet.microsoft.com/enus/library/cc751383.aspx

[36] Campbell, K., Gordon, L.A., Loeb, M.P. and Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. Journal of Computer Security 11 (2003) 431–448 431. IOS Press

[37] Ranking B., (2010). Everything you need to know about Windows. USA: CreateSpace.

[38] Jaikumar, V. (2009). Open source vs pirated operating system. Retrieved from: http://varshamyspace.blogspot.com/2009/01/open-source-vs-pirated-operating-system.html