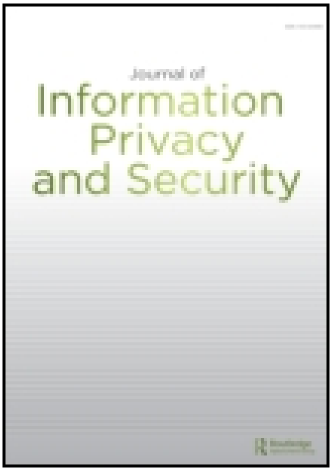


Journal of Information Privacy and Security

Publication details, including instructions for authors and subscription information:
http://www.tandfonline.com/loi/uips20

Students Information Security Practices and Awareness

Ludwig Slusky[a] & Parviz Partow-Navid[b]

[a] California State University - Los Angeles, USA

[b] California State University - Los Angeles, USA

Published online: 07 Jul 2014.

To cite this article: Ludwig Slusky & Parviz Partow-Navid (2012) Students Information Security Practices and Awareness, Journal of Information Privacy and Security, 8:4, 3-26, DOI: 10.1080/15536548.2012.10845664

To link to this article: http://dx.doi.org/10.1080/15536548.2012.10845664

Students Information Security Practices and Awareness

Ludwig Slusky, California State University - Los Angeles, USA
lslusky@calstatela.edu

Parviz Partow-Navid, California State University - Los Angeles, USA
ppartow@calstatela.edu

ABSTRACT

As cyber threats continue to grow at an exponential rate, the need for training in information security awareness spreads far beyond the Information Technology college curriculum. Information Security proliferates into various domains of knowledge and becomes more context-aware. Consequently, the training in information awareness at a college level must cater more specifically to students' practices. This paper presents the results of the Information Security survey conducted among students of the College of Business and Economics at California State University, Los Angeles in spring 2011. The survey revealed several characteristics of students' practices and their awareness of risks and countermeasures related to computer skills, mobile computing, loss and encryption of data, online social networking, awareness training, correlation between practice and awareness, and others. The survey also revealed that the major problem with security awareness is not due to a lack of security knowledge, but in the way the students apply that knowledge in real-world situations. Simply, the compliance with information security awareness is lower than the understanding of it. The findings discussed in this paper are provided to assist colleges in designing curriculum that includes more context-based Information Security training.

KEY WORDS

Cyber Security, Awareness, Risks and Countermeasures, Student Survey

INTRODUCTION

Information technology is a rapidly and significantly changing global economy. Cyber Security threats are becoming more frequent and larger in scope, thus significantly affecting people's life (privacy protection), businesses (information security), and government (homeland security). In fact, Cyber Security, resulted from "the apparent insecurity of the networked global information infrastructure" (ITU, 2005), has grown to become a business itself. Federal Government and States establish Cyber Security agencies and offices. So do Universities: for example, Cyber Security or Information Security offices at Virginia Tech, Georgetown University, Carnegie-Mellon University, University of Louisville, and many others. Colleges and universities store large volumes of students' and employees' sensitive data, including financial records, transcripts, credit histories, medical histories, contact information, social security numbers and other personally identifiable information (Davidson, 2005). A university should provide a forum for easy exchange of information and knowledge. However, students frequently do not safeguard and unintentionally exchange personal information that should be protected. Vulnerabilities, sometimes rooted in a "naïve" student culture, can be observed in students' practices of social networking, sharing passwords and student identification numbers with friends, and not protecting data on mobile devices and media. (Allen, 2011; Cohon, 2009).

President Obama's recent budget proposal for fiscal 2013 identified Cyber Security as "a priority for basic research ... along with clean energy, advanced manufacturing, smart infrastructure and wireless communications." (Jackson 2012). This document emphasizes that "there are a range of emerging threats for which the United States must be prepared, from chemical and biological weapons to cyber-attacks on the nation's critical infrastructure and information technology networks that are integral to our economy and our society."

Academia, business organizations, and government agencies are conducting extensive surveys to gather the views of corporate and individual Information Technology users on the current state of Cyber Security and their recommendations for future priorities and directions. (ISC2, 2010).

Such surveys are indispensable in revealing shortcomings in Cyber Security preparedness. For example, a recent survey (SMB, 2011) of small and mid-sized U.S. businesses revealed that the majority of them are increasingly dependent on the Internet, feel safe from cyber security threats, and yet "almost eighty percent (80%) of them have no formal cyber security policies in place within their organizations." Building Cyber Security awareness and preparedness should start from general education and practices.

Research Hypothesis

Two questions motivated this research: "Are there any significant relationships between students' awareness of risks and other students' characteristics, such as demographics, skills, and practices?" and more specifically "Is there disconnect between students' InfoSec awareness and InfoSec practices?" The hypothesis that the authors operated with was that there are significant correlations in students' Cyber Security behavior among the factors outlined above, and that the practice of Cyber Secure behavior is falling behind the awareness of the risks.

Fisher (2005) points out that "fundamental problems exist with measuring success in security" and that measuring activities vs. accepted benchmarks might provide a solution. Similarly, students' cybersecurity preparedness can be measured by how well cybersecurity practices of students conform to certain accepted benchmarks of awareness.

This paper reports the findings of the Information Security awareness survey of students conducted by the authors in spring 2011. The survey and the corresponding results discussed in this paper present the first attempt to assess basic Information Security knowledge and skills of students based on a sample group mostly comprised of students from the College of Business and Economics (CB&E), California State University, Los Angeles (CSULA). The follow-up surveys will be at an expanded level of depth and breadth of students' InfoSecurity knowledge and practices.

Information Security Issues for Students

Throughout college years, students leave a significant "digital footprint" visible to others about their personal and academic life. As a result, their privacy is very much at risk (Mills, 2008).

College admissions officers and potential employers check online information sources (online social networks, individual students' websites, and other) about applicants in considering whether or not to admit or hire them.

Teaching faculty frequently checks students' records and communicates privileged information (names and campus identification numbers, grades, etc.) with students over email and websites. Also, a professor may retain intellectual work of students (with embedded personal information) on a learning management system (e.g., Moodle, Blackboard) or in his/her private repository with no defined expiration date.

Students form virtual (online) teams using cloud computing (e.g., Google Docs), where they may disclose some privileged information about themselves or others. They increasingly communicate over text messaging and Twitter rather than via phone. They also create personal social networks online. They may have misconception about how long the records they created online will be retained by the service provider.

Often students are suggested to do their class projects using a place of work as the example. Without realizing so, the students may violate laws or his/her employer's regulations when disclose organization's privileged information in their projects.

Much of the students' privileged information may be revealed inadvertently with lost or stolen flash drives or mobile computing devices.

In cases, when a student is a hacking perpetrator, personal and academic records of other students are at risk. Students with advanced know-how in Cyber Security issues are not restricted by the "need to know" principle and may be motivated to discover personal information of others.

There are several initiatives and organizations focused on protecting students' privacy. The Family Educational Rights and Privacy Act (FERPA) is a Federal law that protects the privacy of student education records (UC Davis, 2008). But the best defense in protecting identity, privacy, and future opportunities for a student is to raise his/her Cyber Security awareness (that includes understanding of applicable laws) and make it actionable, i.e., implements it in practice.

In addition to each campus' Information Assurance efforts, there are several national and international organizations (e.g., ISC^2, GIAC, CompTIA), certificate programs (e.g., CISSP, GIAC Security, Security+), and numerous publications (Harris, 2013) to assist faculty and students with understanding of various Information Security issues.

Survey Questions Mapping

Survey Scope

The purpose of the survey was to review information security practices and risks arising from students' use of computers and countermeasures for data protection on campus or at home. The categories of questions in the survey included: student academic profile, Information Technology (IT) resources, IT skills, experience with loss of data, awareness of risks, and awareness of countermeasures. The last two categories were used with conventional risk analysis based on the likelihood and the impact of an occurrence.

The survey was conducted in various classes of the CB&E during regular class sessions and was supervised by the instructors of those classes. CSULA is an urban learning institution with about 3,000 undergraduate and 300 graduate students. CSULA primarily serves as a commuter and night university for many working people in Los Angeles. A unique characteristic of CSULA is its diverse student body, a significant percentage of which is of Latino heritage.

The survey used a non-representative sample of the CB&E population under study. In total, 397 graduate and undergraduate students were randomly selected for the survey. The participants were given 30 minutes to complete and submit the survey. All collected survey forms were evaluated for completeness; as a result, the total number of usable responses received was reduced to 340.

Survey Instrument Design

Information Security awareness is a multifaceted topic. Surveying all aspects of it together in one survey would present a logistical problem. The key to developing this survey instrument was to keep it short provided that the essential information needed for the research purpose would be obtained.

The survey instructions outlined the purpose and explained how to answer the questionnaire. The questionnaire form was designed for maximum efficiency given the constraint of time (20-30 minutes) and length (a single double-sided page).

The survey was designed to obtain data about demographics, IT resources and skills, risks and countermeasures (with data loss as a sub-group). The guiding models (Groves, 2009) considered in designing the Information Security survey were Cognitive Model and System Model of the IT user. The survey used the cross-sectional method to collect data about students' characteristics at a single point in time and used two types of measurement scales (Monash, 2012):

- Nominal type – two-point scale (e.g., Yes/No scale, Male/Female).
- Interval type – a four-point scale (low, moderate, significant, high), the five-point Likert scale (from Strongly Disagree to Strongly Agree), a six-point scale (from Very Poor to Excellent), a nine-point scale (from 0-10 hrs to 46+ hrs), and others.

The survey was interviewer-administered using a paper form with closed-end questions; no incentives were offered to participants for completing the survey.

The questions in the survey were written with consistency, leaving no gaps between response choices and not leading students to what the authors would perceive as a "preferred choice answer" by stating that answer differently from the others. The questions were formulated to be short and concise, in unbiased way and were presented in the survey form in an organized layout where the questions were grouped by categories.

In total, the survey had 29 questions organized in 3 categories (Skills, Practices, and Awareness) and 5 sub-categories. Figure 1 shows mapping of the categories and sub-categories in the survey. Here, categories InfoSecurity Practices and Impact Awareness share the same sets of questions (Risks and Awareness) in the survey.

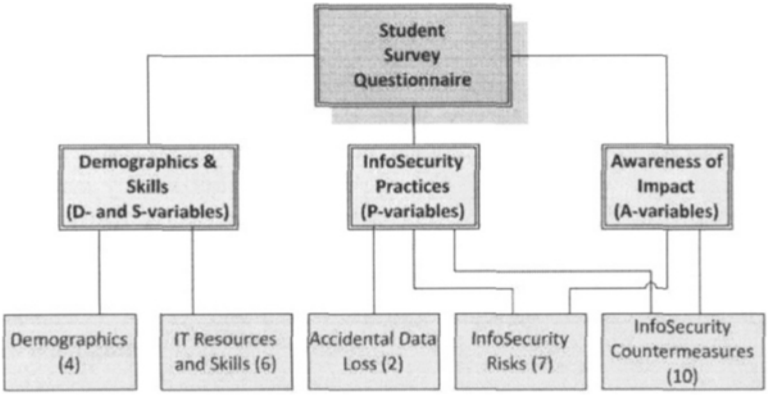

Student Survey Questionnaire
Demographics & Skills (D- and S-variables)
InfoSecurity Practices (P-variables)
Awareness of Impact (A-variables)
Demographics (4)
IT Resources and Skills (6)
Accidental Data Loss (2)
InfoSecurity Risks (7)
InfoSecurity Countermeasures (10)

Figure 1. Survey Questions Mapping (with number of questions)

The questions were numbered sequentially and denoted by a related category indicator as S-variables for skills, P-variables for practices, and A-variables for awareness. The first sub-category profiled academic characteristics of students (questions 1 through 4). The second sub-category of questions was focused on students' IT skills and resources (questions 5 through 10). The third sub-category of questions inquired about participants experience with loss of data (questions 11 and 12). The remaining fourth and fifth sub-categories assessed participants' views about various risks (sub-category 4, questions 18 and 19) and countermeasures (sub-category 5, questions 20 through 29) from two angles: (a) having risks encountered or countermeasures employed in practice, and (b) being aware of the significance of these risks and countermeasures.

Risks resulting, for example, from inappropriate use of passwords and online accounts and countermeasures (such as acceptable use policy, encryption, and antivirus) were selected among those that are typical for students' on-campus and home computing environment.

Analysis Tools

The collected survey results were reviewed for any missing data and entered into SPSS Statistics software for further analysis. The basic methods of the analysis were SPSS Descriptive Statistics tools (Frequencies, Descriptive, and Cross Tabulation) and Pearson Bivariate Correlation for selected variables.

Statistical analysis with Descriptive data included Minimum, Maximum, Mean, and comparison of means for identified data items. Deviation parameters and Bivariate Correlation included data items (responses in the surrey) that participated in statistically significant correlations. Summary of the significant findings from this analysis are presented below.

RESPONDENTS' PROFILE

Demographics Data

The first 4 questions of the survey were designed to collect information on the respondents' profile. Personal or demographic information (age, race, native language, etc.) are typically not welcomed by the respondents. This survey limited the profile information to absolute minimum of four data items necessary for the research; they included gender, major, class level, and overall GPA. Table 1 below shows respondents' profiles data.

Table 1. Respondents' Profile: Demographics Data

D#	Demographics: Profile Data									
D1	**Gender**	*Male*	*Female*							
		57.6	42.4							
D2	**Major**	*ACCT*	*ECON*	*FIN*	*LAW*	*CIS*	*MGMT*	*MKT*	*Other*	*U/D**
		13.5	2.9	11.2	1.2	12.4	31.8	15.6	10.3	1.2
D3	**Class Level**	*Freshman*	*Sophomore*	*Junior*	*Senior*	*Grad*	*Other*			
		2.6	7.6	43.5	35.6	3.8	6.5			
D4	**Overall GPA**	*Less than 2.0*	*2.0-2.2*	*2.3-2.5*	*2.6-2.8*	*2.9-3.1*	*3.2-3.4*	*3.5-3.7*	*3.8-4.0*	*None*
		1.8	7.6	13.8	17.9	22.1	17.9	12.9	5	0.9

*U/D – Undecided

** D# - Variables relate to DEMOGRAPHICS category

The majority of the respondents (about 80%) were upper class undergraduate students. The largest group (above 30%) comprised students with major in Management major; close to 77% of the respondents had GPAs above 2.5. The headcount of the surveyed sample group by gender differs significantly from the general student population at the University (CSULA), but, as displayed in Figure 2, it is closer to the ratio of the College (CB&E) where the sample group came from.

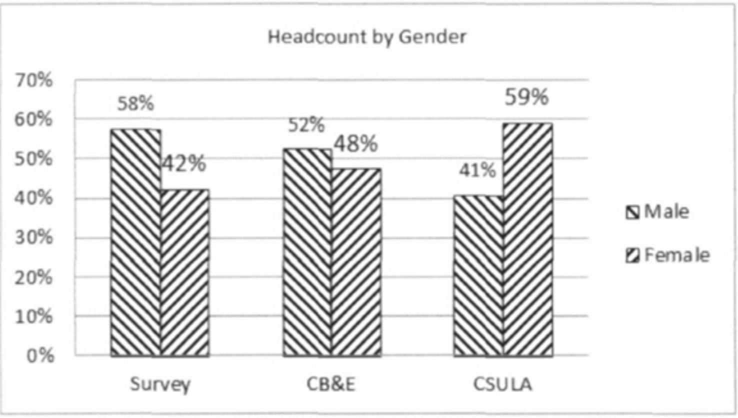


Figure 2. Headcount of Students by Gender

Although the question of age was not explicitly asked in the survey, the generational cohort of the entire sample can be characterized as upper-bound lattice of Generation Y (those born 1977-1994). The overwhelming majority of the students in the sample were juniors and seniors.

Grade Point Average (GPA)

The survey data shows that the mean GPA varied insignificantly among majors - within the range of 2.8 - 3.1 (the margin of error: +/- 0.1) with exception of one students' group (LAW) which was too small to establish any pattern. Actual distribution of the mean GPA is shown in Table 2.

Table 2. GPA (Mean) by Major

Major	ACCT	ECON	FIN	LAW	CIS	MGMT	MKT	Other
GPA (Mean)	2.8	3.1	3.1	3.7**	3.0	3.0	2.9	2.9

*Margin of error: +/- 0.1

** Non-representative small set of students

The distribution of GPA per Gender (mean value) varied slightly – it was 3.78% higher for male students. The GPA per Class Level (mean value) varied more noticeably, within the range of 2.9 - 3.4 (the margin of error: +/- 0.1) with the highest at the freshman level and the lowest at the Junior and Senior levels. As Table 3 shows, the actual distribution of the mean GPA by class level declined for junior and senior students, who represented the bulk of the survey sample group.

Table 3. GPA (Mean) by Class Level

Class Level	Freshman	Sophomore	Junior	Senior	Graduate	Other
GPA (mean)	3.2	3.0	2.9	2.9	3.0	3.4

*Margin of error: +/- 0.1

It's noteworthy that the distribution of GPA by frequencies within the survey sample group (as seen in the Figure 3) has a clear inverted V-shape.

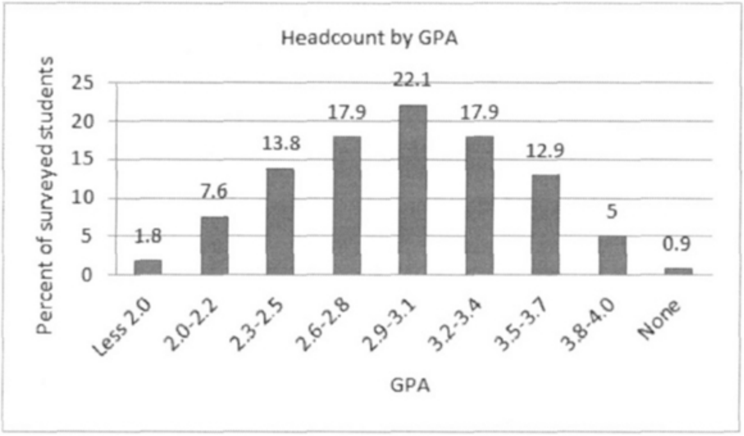


Figure 3. Headcount by Grade Point Average (GPA)

Information Technology Resources and Skills

The types of available computers and the level of computer skills are fundamental to the Information Security. Table 4 shows distribution frequency (in %) of responses to the next six survey questions (5 thru 10) in the category Skills.

PASW statistical analysis showed statistically significant Pearson Correlations among four D-variables and six S-variables (see Table 5).

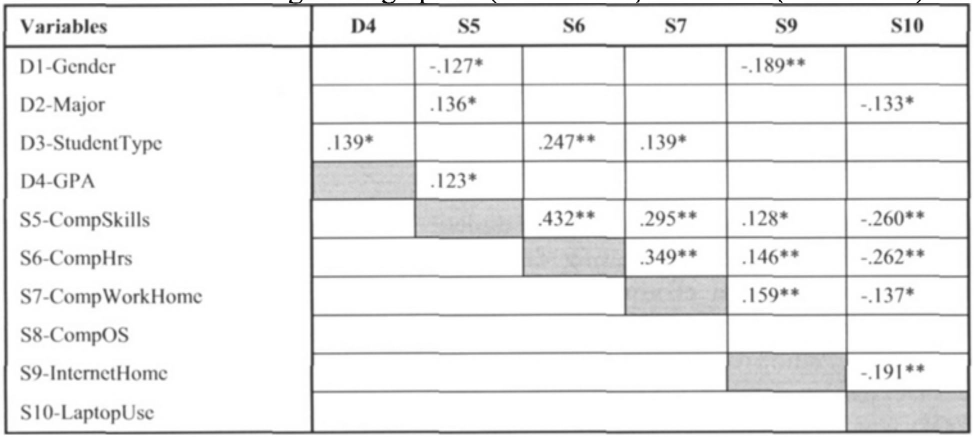
Table 4. Students' IT Resources and Skills (%)

S#	***Category Skills: IT Resources and Skills***									
S5	My computer skills are …	Very Poor	Inadequate	Average	Good	Very good	Excellent	N/A**		
		0.6	3.8	20.9	29.7	30.2	14.5	0.3		
S6	I use a computer… hours/week	0-10 hrs	11-15 hrs	16-20 hrs	21-25 hrs	26-30 hrs	31-35 hrs	36-40 hrs	41-45 hrs	46+ hrs
		8.5	11.2	12.1	15.9	7.6	10	12.4	5.3	17.1
S7	I use computers mostly for …	Study	Work	Social	Study & work	N/A**				
		18.5	6.2	15.6	59.4	0.3				
S8	My home computer …	Windows	Mac	Other	None					
		82.4	15.3	1.5	0.9					
S9	My Internet access at home is …	Wired	Wireless	Both	None					
		7.4	57.4	34.7	0.6					
S10	I frequently use my laptop on Campus	Yes	No	N/A**						
		55.3	44.4	0.3						

* S# - skills are denoted as S-variables related to SKILLS category

**N/A – Not answered

Table 5. Correlation among Demographics (D-variables) and Skills (S-variables)



Variables	D4	S5	S6	S7	S9	S10
D1-Gender		-.127*			-.189**	
D2-Major		.136*				-.133*
D3-StudentType	.139*		.247**	.139*		
D4-GPA		.123*				
S5-CompSkills			.432**	.295**	.128*	-.260**
S6-CompHrs				.349**	.146**	-.262**
S7-CompWorkHome					.159**	-.137*
S8-CompOS						
S9-InternetHome						-.191**
S10-LaptopUse						

* Correlation is significant at the 0.05 level (2-tailed)

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

*** Only Statistically Significant Correlations are shown here

Computer Skills

Among *Skills* variables, the *Computer Skills* variable S5 is the predominant factor for assessment of the information security practices and awareness. Significance of such correlations is discussed and illustrated in the diagrams below.

A majority of students, about 95%, believed that they have average or better than average computer skills, and about 60% of the students assessed themselves in two (out of six) categories as having Good or Very Good computer skills (Table 4, S5). About 70% of students used computers for more than 20 hours per week. Close to 60% of students have been using computers both for study and work. Internet availability at home reached almost 100%; only 0.6% of the students indicated no access to the Internet at home. Among Operating Systems (OS) that they used, Microsoft Window – at 82.4% - remained the dominant OS.

Cross tabulation of Computer Skills levels with Computer Hours (see Figure 4) shows an average increase of 5 hours in weekly computer usage as computer skills advance from Average to Excellent levels.

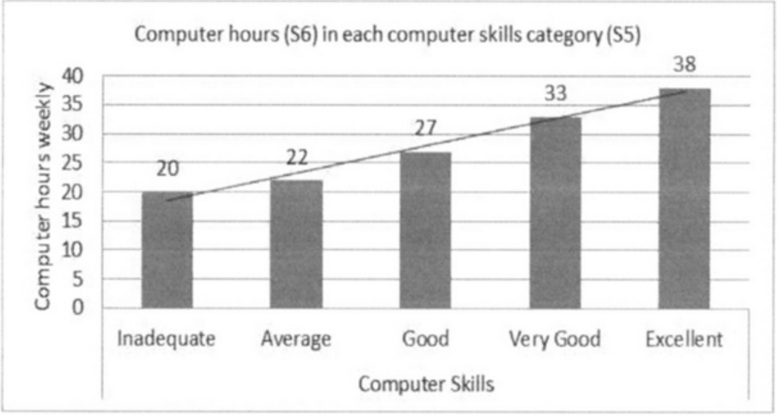


Figure 4. Computer Usage (Hours Weekly) and Computer Skills

Mobile Computing

Mobile computing becomes vital for students' studies on campus and at home. Researchers are now investigating and promoting use of computer tablets with wireless capabilities in classrooms. More students bring computers with them to campus as their computer skills improve. Figure 5 shows close to linear progression of the percent of students in each computer skills category that use BYOD (Bring Your Own Device) on campus for their studies. The average percent of students practicing BYOD was 55% across all categories and reached 67% or higher for students with very good or excellent computer skills.

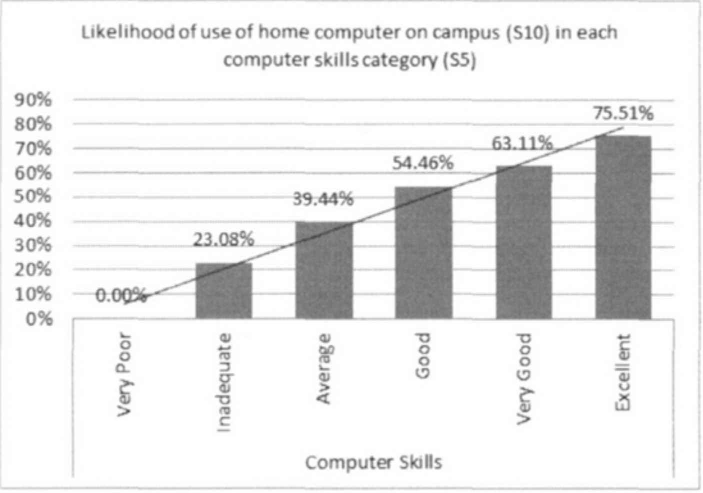


Figure 5. Usage of Home Computers on Campus and Computer Skills

INFORMATION SECURITY PRACTICES AND AWARENESS

Practice and Awareness Variables

Tables 6, 7, 8, 9, and 10 below summarize practice variables (P-variables) and awareness variables (A-variables). Practice variables are grouped into three categories: loss of data, risks, and countermeasures. Awareness variables indicate students' awareness of the potential impact that risks and countermeasures may have.

Table 6. Students' Data Loss Experience (%)

P#	Loss of Data	Yes	No	N/A**
P11	My laptop was lost or stolen	3.2	96.8	
P12	My flash drive was lost or stolen	11.2	88.5	0.3

* P# - practices are denoted as P-variables
**N/A – Not answered

Table 7. Students' Practice Risks: Loss of Data or Privacy (%)

P#	Risks in Practices: Data and Privacy Vulnerabilities	Risks Acceptance (%)				
		Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
P13	Online social networks that I use provide all necessary protection of my personal data	11.2	22.6	30.3	26.5	9.4
P14	If my online account is protected then it is safe to use it from public computers (work, campus, WiFi zone)	9.4	23.5	22.4	37.1	7.6
P15	Online social networks will purge data in my account after a few years of inactivity	8.2	17.6	45	25.9	3.2
P16	I can give up some privacy of my personal data for increased convenience of public Web access	18.5	32.1	21.5	24.1	3.8
P17	I am at risk that my laptop or flash drive with my data files can be lost or stolen on campus	9.7	17.1	24.1	35	14.1
P18	Same passwords for several online accounts is safe	32.9	32.1	18.5	15.3	1.2
P19	Sharing passwords with trusted college friends is safe	55	26.5	10.9	6.5	1.2

* Some fractional data is omitted; the total percentage may be less than 100%

Table 8. Students' Practice Countermeasures: Loss of Data and Privacy Prevention(%)

P#	Countermeasures in Practices: Prevention of loss of data and privacy	Countermeasures Acceptance (%)				
		Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree
P20	CSULA Acceptable Use Policy ("Responsible Use of Information Technology") helps protecting my data	5.6	13.5	44.4	31.2	5.3
P21	I have sufficient knowledge of Information security	4.7	16.5	29.7	41.2	7.9
P22	Best online practices will completely protect my data	10	26.2	31.8	25.6	6.5
P23	I have encrypted many data files on my computer	11.8	24.4	35	22.6	6.2
P24	I should have all my private data files encrypted when I bring them to campus on a laptop or a flash drive	3.8	12.6	32.1	40.6	10.9
P25	Deleting files from the recycle folder in the computer completely erases these files	26.8	29.4	15.3	22.9	5.6
P26	I regularly maintain backup of my personal files	6.2	23.5	18.8	39.1	12.4
P27	I am satisfied with anti-virus software I use	5	14.4	23.8	42.6	14.1
P28	I would prefer new Google-based PCs for the Cloud Applications vs. my traditional computer (where I need to install applications) if the applications are the same	7.9	17.4	34.7	30.3	9.7
P29	I would participate regularly in a 15-min semiannual online Information Security Awareness Update program	12.1	20.6	29.8	28.8	9.7

* Some fractional data is omitted; the total percentage may be less than 100%

Table 9. Awareness of Risks: Losing Data or Privacy (%)

A#	**Awareness of Risks:** Data and Privacy Vulnerabilities	**Awareness of Potential Impact of These Risks (%)**			
		Low	Moderate	Significant	High
A13	Online social networks that I use provide all necessary protection of my personal data	5	22.1	34.4	38.2
A14	If my online account is protected then it is safe to use it from public computers (work, campus, WiFi zone)	4.4	18.5	35.6	40.9
A15	Online social networks will purge data in my account after a few years of inactivity	6.5	30	32.4	30.9
A16	I can give up some privacy of my personal data for increased convenience of public Web access	5	25	31.5	37.9
A17	I am at risk that my laptop or flash drive with my data files can be lost or stolen on campus	5.9	17.9	32.1	43.5
A18	Same passwords for several online accounts is safe	4.4	20.9	29.7	44.1
A19	Sharing passwords with trusted college friends is safe	5.3	20	27.6	46.2

* Some fractional data is omitted; the total percentage may be less than 100%

Table 10. Awareness of Countermeasures: Loss of Data or Privacy Prevention (%)

A#	**Awareness of Countermeasures:** Prevention of loss of data and privacy	**Awareness of Potential Impact of these countermeasures (%)**			
		Low	Moderate	Significant	High
A20	CSULA Acceptable Use Policy ("Responsible Use of Information Technology") helps protecting my data	7.9	27.9	30.9	32.6
A21	I have sufficient knowledge of Information security	4.4	22.1	37.9	35
A22	Best online practices will completely protect my data	4.1	25.6	34.4	35.3
A23	I have encrypted many data files on my computer	6.5	25	33.8	33.8
A24	I should have all my private data files encrypted when I bring them to campus on a laptop or a flash drive	5.6	25	35	33.5
A25	Deleting files from the recycle folder in the computer completely erases these files	6.5	26.2	32.4	32.9
A26	I regularly maintain backup of my personal files	4.4	21.2	32.4	40.9
A27	I am satisfied with anti-virus software I use	3.5	19.7	34.1	41.8
A28	I would prefer new Google-based PCs for the Cloud Applications vs. my traditional computer (where I need to install applications) if the applications are the same	11.8	25.9	27.1	34.4
A29	I would participate regularly in a 15-min semiannual online Information Security Awareness Update program	12.6	27.1	29.1	30.3

* Some fractional data is omitted; the total percentage may be less than 100%

P-variables and A-variables were rated with two different scales (five-point scale for P-variables and four-point scale for A-variables) next to each other in the same section of the questionnaire (see Table 11). The survey's classification of A-variables is similar to the suggestion of the Red Hat Security Response Team (RedHat, 2012) to rate the impact of security issues using a four-point scale (low, moderate, important, and critical).

Table 11. Scales for P-variables and A-variables Values

P-variable Value	
Value	Value name
5	Strongly Agree
4	Agree
3	Neither Agree nor Disagree
2	Disagree
1	Strongly Disagree

A-variable Value	
Value	Value name
4	High
3	Significant
2	Moderate
1	Low

Loss of Data

Loss of data is one of the most significant vulnerabiliticse for students; it usually comes with use of portable and mobile IT technology. Two types of IT devices surveyed here were laptops and flash drives. Table 6 above illustrates the students' experience in this area. About 3% of the respondents had lost their laptops at least once. And, 11% of the surveyed students had their flash drives lost or stolen. That is significantly lower than in the survey conducted by FBI (2005), 15.5% of the respondents indicated loss of a laptop, PC, or PDA. The actual of data loss by students through lost or stolen flash drives varies with computer skills as illustrated in the Figure 6 below.

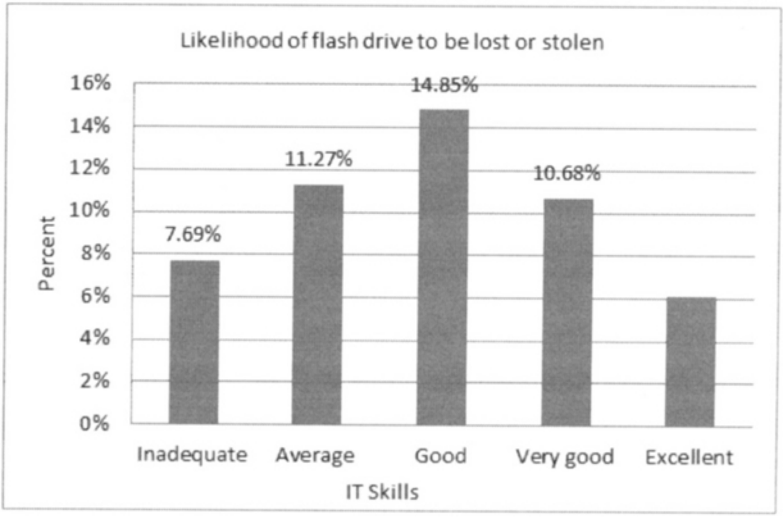


Figure 6. Lost Flash Drive Data by Categories of Computer Skills

The highest percent of students whose flash drive was lost or stolen (see Table 6, P12) was in the category of students with GOOD computer skills (see Figure 6 above); it is significantly higher than in the categories of students with lower (Inadequate or Average) or higher computer skills (Very Good or Excellent). One explanation for this phenomenon is that the students with GOOD computer skills tend to use flash drive to transport data much more frequently than the students of lower skills categories do, but they are lacking the expertise that the upper students have.

The percent of students whose laptops were lost or stolen is only 3.2% and is not significant enough to compare by skills, although there is a small indication (not statistically confirmed) that the students with VERY GOOD computer skills are much more careful - only 1% of them reported lost or stolen computers.

Perceived risk of BYOD or flash drives to be lost or stolen on campus differs from actual losses reported by students (P11 and P12) and discussed above (Table 6). Almost 49% of the students agree or strongly agree that they are at risk of having their laptop or flash drive lost or stolen on campus (Table 7, P17), while about 75% of them believe that the potential loss resulted from this risk factor would be significant or high (Table 9, A17).

Data Encryption and Passwords

It is noteworthy, that among all Practice variables for risks (PA13-PA19) and countermeasures (PA20-PA29) listed in Tables 7 and 8, the variable P24 (data encrypted when brought to campus) showed the highest consistent and statistically significant correlation with corresponding Awareness variables in the same sub-categories (A13 through A29); it ranged from .314** to .746** (** Correlation is significant at the 0.01 level, 2-tailed). It points to practicing data encryption as an important indicator of the overall Information Technology awareness for students.

Sharing passwords is another important characteristic. Not surprisingly, there is a strong correlation of 0.455** (** correlation is significant at the 0.01 level, 2-tailed) between variables P18 (sharing a password among friends) and P19 (sharing a password among online accounts), both listed in Table 7. Majority of the students were consistent in giving responses to both questions.

About 60% of students strongly or moderately rejected (disagreed with) both statements; the rest of the students showed neutrality or some acceptance of either P18 or P19 statements. Thus, 40% of students indicated less than satisfactory information security practices of protecting passwords from sharing among online accounts and friends. This is consistent with the Cyber Security Alliance report (September 2011) that concludes that 46% of 18-24 year olds are using file sharing programs that allows other people access their files and programs.

Risks of Online Social Networking

Variables P13 thru P19 in Table 7 show students' responses to the risks of losing data and privacy. Only 35.9% of students agree or strongly agree that online social networks provide all the needed protections (Table 7, P13), while about 72.6% of students were aware that security issues of online social networks have a significant or highly significant impact on their privacy (Table 9, A13).

Somewhat similar results were received about students' practices and their awareness of the risks associated with use of public computers to access protected online accounts (Table 9, A14 and Table 7, P14). A large majority of students indicated the significance of these risks as significant or high (76.5% in Table 9, A14). And, only 44.7% of them agree or strongly agree that it is safe to use their accounts from public computers (Table 7, P14).

About 30% of students believed (moderately or strongly) that the online social networks will purge their data after a few years of inactivity (Table 7, P15) and twice as much (about 63%) of the respondents rated this issue as significant or highly significant (Table 9, A15).

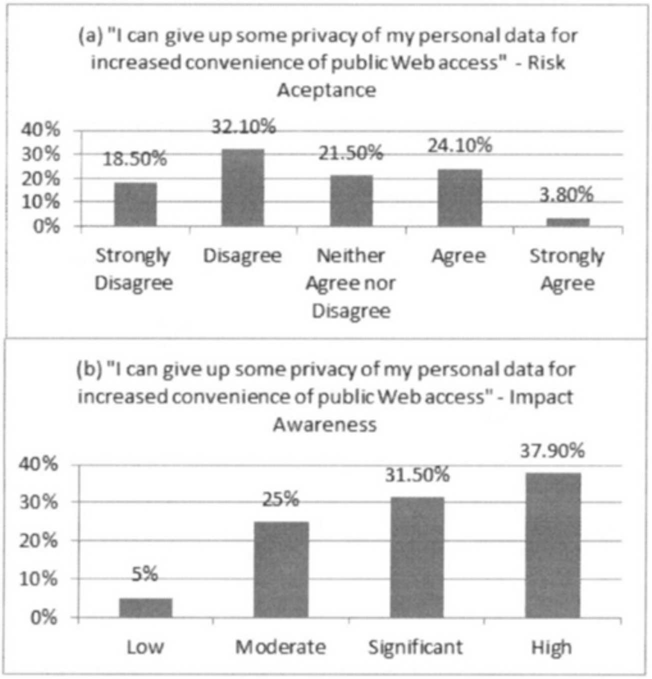


Figure 7. Privacy Protection vs. Convenience of Public Web Access
(a) Risk Acceptance P16; (b) Awareness of Impact A16

Online privacy vs. online convenience was investigated in question 16. Here, only about 28% of the students agreed or strongly agreed to give up some privacy for increased convenience of public web access (see Table 7, P16), while almost 70% of students were aware that it would present a significant or high security risk (Table 9, A16). Such inconsistency was found among almost all students: from those who strongly oppose reduction of privacy protection to those who strongly agree with it (see Figure 7 below).

It is also noticeable that the students with average computer skills displayed slightly less recognition of risks associated with such trade-offs than the students with excellent or poor computer skills (see Figure 8 below).

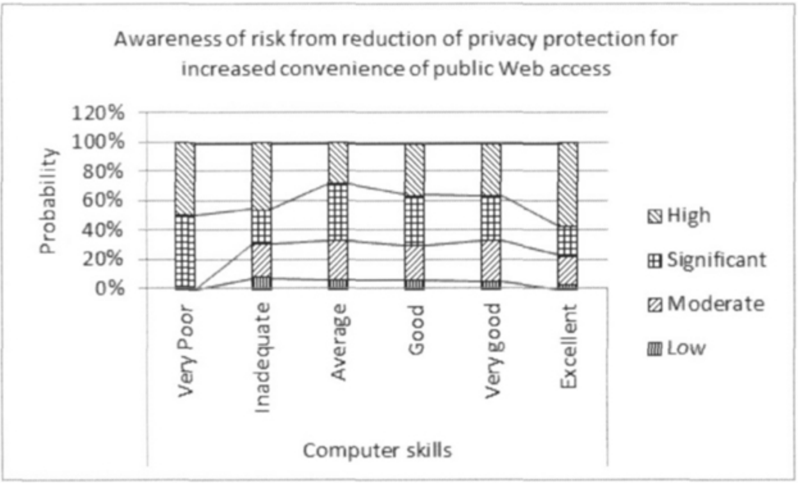


Figure 8. Trade-off of Privacy Protection vs. Convenience of Web Access (A16) and Computer Skills (S5)

Information Security Awareness Training

About 60% of students realize the importance of an Information Security Awareness training as significant or high (Table 10, A29), but only about 40% of them would certainly participate in a 15-min semiannual online Information Security Awareness program (Table 8, P29).

Averaging Responses

The average students' responses to questions on the existence of risks and countermeasures in practice and the average students' awareness of the potential impact of these risks and countermeasures can help assess the overall level of students' information security preparedness. Tables 7 to 10 above illustrate this point.

The P-variable Average (PVA) values for risks (P13-P19) and countermeasures (P20-P29) in students' practices are shown separately in the Figure 9 and Figure 10 accordingly.

Figure 9 shows that the average students' recognition of the defined risks in their practices fluctuates for the most part from "rejection" of risk ("Disagree") to "neutral" ("Neither Agree nor Disagree").

The highest (but still at the "neutral" level) realized risk (as measured by PVA) was demonstrated by students' responses to the survey statement P17: "I am at risk that my laptop or flash drive with my data files can be lost or stolen on campus." On the opposite side, the lowest (slightly below the "rejection" level) realized risk was demonstrated by responses to the statement P19 "Sharing passwords with trusted college friends is safe."

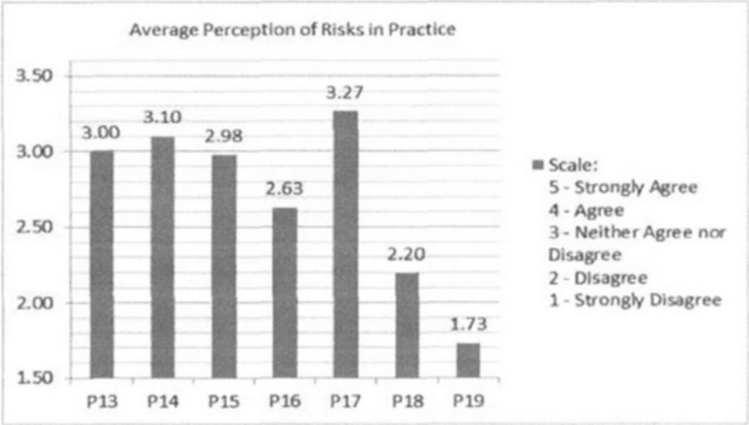


Figure 9. P-variable Average (PVA) Values for Risks in Practice
* Scale levels 4 to 5 are not shown

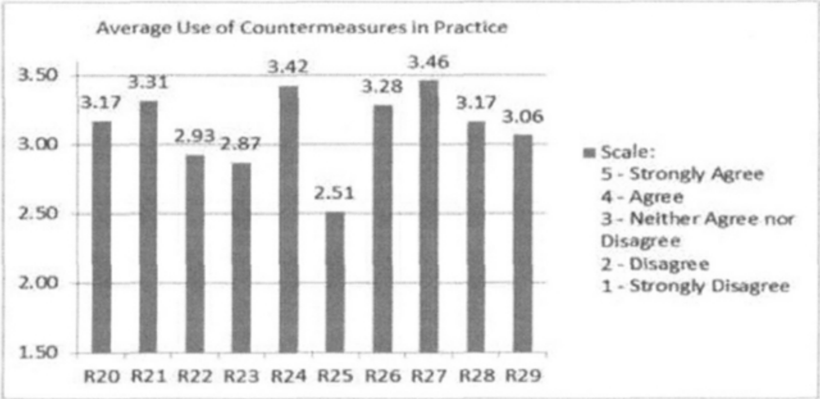


Figure 10. P-variable Average (PVA) Values for Countermeasures in Practice
* Scale levels 4 to 5 are not shown

The A-variable Average (AVA) values for awareness of potential impact of risks (A13-A19) and countermeasures (A20-A29) are shown in the Figure 11 and Figure 12 below. The AVA averages show more uniformity in responses, all at or about "significant" level.

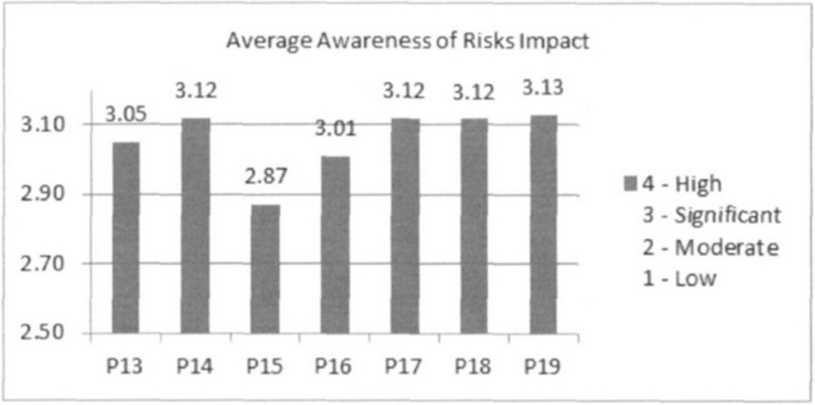


Figure 11. A-variable Average (AVA) Values for Risks Impact Awareness
* Scale level 4 is not shown

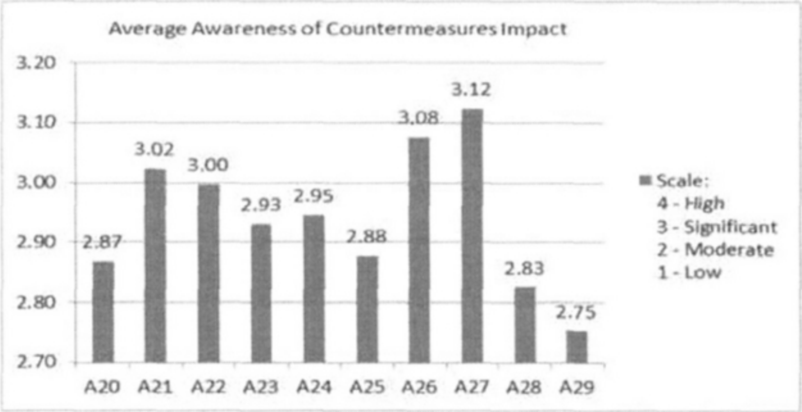


Figure 12. A-variable Average (AVA) Values for Countermeasures Impact Awareness
* Scale level 4 is not shown

Correlation between Practice and Awareness

The correlation between students' practices of information security and their awareness of the potential impact of risks and countermeasures was not always consistent. Thus, analysis of the survey data showed that the Pearson Correlation only among A-variables is statistically significant, thus confirming that there is coherence in students' awareness of information security issues (see Table 12).

Table 12. Correlation Coefficients among A-variables

Awareness Variables	A13	A14	A15	A16	A17	A18	A19	A20	A21	A22	A23	A24	A25	A26	A27	A28	A29
A13-SocNetwork		.683**	.620**	.567**	.494**	.484**	.453**	.609**	.577**	.503**	.517**	.149**	.503**	.438**	.476**	.466**	.456**
A14-AcctProtect			.603**	.558**	.557**	.512**	.501**	.574**	.567**	.516**	.567**	.148**	.496**	.439**	.481**	.454**	.495**
A15-PurgeData				.619**	.554**	.523**	.454**	.562**	.613**	.538**	.630**	.167**	.501**	.452**	.523**	.508**	.534**
A16-Privacy					.670**	.557**	.543**	.515**	.579**	.517**	.595**	.260**	.427**	.491**	.480**	.476**	.498**
A17-DataLost						.568**	.504**	.514**	.521**	.567**	.568**	.277**	.529**	.492**	.516**	.506**	.469**
A18-SamePSW							.750**	.467**	.489**	.539**	.515**	.188**	.500**	.491**	.474**	.364**	.404**
A19-SharePSW								.408**	.411**	.406**	.479**	.136*	.465**	.484**	.381**	.324**	.418**
A20-UsePolicy									.710**	.650**	.635**	.182**	.527**	.493**	.489**	.572**	.569**
A21-KnowledgeLvl										.698**	.684**	.188**	.551**	.604**	.603**	.557**	.572**
A22-BestPractice											.692**	.184**	.608**	.565**	.609**	.638**	.550**
A23-EncryptionHome												.288**	.652**	.613**	.578**	.602**	.603**
A24-EncryptCampus													.122*	.127*	.128*	.168**	.152**
A25-DeleteSafe														.643**	.517**	.516**	.552**
A26-Backup															.628**	.591**	.575**
A27-AntiVirus																.517**	.574**
A28-CloudApps																	.698**
A29-Training																	

* Correlation is significant at the 0.05 level (2-tailed)

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

However, the correlations among P-variables were sporadic, not consistent, pointing to a lack of coherence in students' practices of information security (see Table 13). Furthermore, the correlations between P-variables and A-variables (see Table 14) were also sporadic, not consistent, except for three P-variables: P19 (Share password), P24 (Encryption on campus), and P29 (Awareness training). Significant correlations of these P-variables with many Awareness variables means that overall the students applied what they know about these factors in their practices.

Table 13. Correlation Coefficients among P-variables

Practice Variables	P13	P14	P15	P16	P17	P18	P19	P20	P21	P22	P23	P24	P25	P26	P27	P28	P29
P13-SocNetwork		.483**	.304**			.159**	.135*	.188**		.266**			.244**			.148**	
P14-AcctProtect			.236**	.124*		.151**	.135*	.353**	.190**	.340**	.138*		.262**		.150**	.233**	
P15-PurgeData				.167**	.183**		.151**	.249**	.153**	.289**	.277**		.211**	.142**		.177**	
P16-Privacy						.108*	.255**	.188**				-.129*	.149**				
P17-DataLost																	
P18-SamePSW							.455**			.227**			.254**				
P19-SharePSW								.111*		.178**	.139*	-.134*	.234**				
P20-UsePolicy									.295**	.331**	.281**		.198**		.166**	.268**	
P21-KnowledgeLvl										.313**	.393**			.285**	.307**	.150**	.150**
P22-BestPractice											.368**		.286**	.147**	.188**	.175**	
P23-EncryptionHome													.124*	.285**	.235**	.155**	.169**
P24-EncryptCampus																	.184**
P25-DeleteSafe															.202**	.247**	
P26-Backup															.271**		.243**
P27-AntiVirus																	
P28-CloudApps																	.155**
P29-Training																	

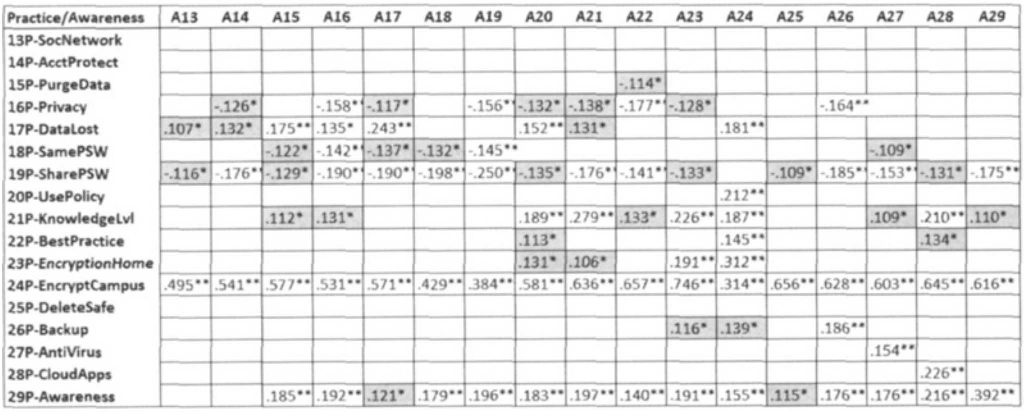
* Correlation is significant at the 0.05 level (2-tailed)

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

*** Only Statistically Significant Correlations are shown here

A lack of coherence between the majority of P-variables and A-variables leads to the conclusion that the focus of Information Security training for students should not be exclusively on building Information Security knowledge to elevate awareness; but rather it should be on the linkage between awareness and practices. It does not mean that training in the Information Security knowledge is less important; on the contrary, it means that any such training should be focused on knowledge re-enforcing practice, not merely knowledge.

Table 14. Correlation Coefficients between P-variables and A-variables



Practice/Awareness	A13	A14	A15	A16	A17	A18	A19	A20	A21	A22	A23	A24	A25	A26	A27	A28	A29
13P-SocNetwork																	
14P-AcctProtect																	
15P-PurgeData										-.114*							
16P-Privacy		-.126*		-.158**	-.117*		-.156**	-.132*	-.138*	-.177**	-.128*			-.164**			
17P-DataLost	.107*	.132*	.175**	.135*	.243**			.152**	.131*			.181**					
18P-SamePSW			-.122*	-.142**	-.137*	-.132*	-.145**								-.109*		
19P-SharePSW	-.116*	-.176**	-.129*	-.190**	-.190**	-.198**	-.250**	-.135*	-.176**	-.141**	-.133*		-.109*	-.185**	-.153**	-.131*	-.175**
20P-UsePolicy												.212**					
21P-KnowledgeLvl			.112*	.131*				.189**	.279**	.133*	.226**	.187**			.109*	.210**	.110*
22P-BestPractice								.113*				.145**				.134*	
23P-EncryptionHome								.131*	.106*		.191**	.312**					
24P-EncryptCampus	.495**	.541**	.577**	.531**	.571**	.429**	.384**	.581**	.636**	.657**	.746**	.314**	.656**	.628**	.603**	.645**	.616**
25P-DeleteSafe																	
26P-Backup											.116*	.139*		.186**			
27P-AntiVirus															.154**		
28P-CloudApps																.226**	
29P-Awareness			.185**	.192**	.121*	.179**	.196**	.183**	.197**	.140**	.191**	.155**	.115*	.176**	.176**	.216**	.392**

* Correlation is significant at the 0.05 level (2-tailed)

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

*** Only Statistically Significant Correlations are shown here

Among all P-variables, one that consistently exhibited statistically significant correlation with the A-variables was P24 - a statement of need to have private data files encrypted when a student brings them to campus on BYOD or a flash drive. Not surprisingly, the students who strongly agree with the need for data encryption (P24) are the most likely (close to "High" with the weight 3.81) to realize that BYOD or a flash drive with data files can be lost or stolen on campus (A17). Accordingly, the students who strongly disagree with the need for data encryption on campus are also among the least likely (the weight 2.85) to realize the importance of regular data backup (A26). Overall, the students who strongly agree with the need for data encryption are aware of other risks and countermeasures (A13 to A29) in the significant-to-high range.

Among all surveyed risks and countermeasures, awareness of Information Security periodical training (A29) on average was the lowest followed by uncertainty about the security of cloud applications (A28), data purge from online social networks (A15), and Acceptable Use Policy (A20). Contrary to that, the highest awareness of risks and countermeasures was demonstrated on the issues of sharing passwords (A19), use of anti-virus software (A27), and risks of data loss (A17).

CONCLUSION

As cyber threats continue to grow at an exponential rate, the need for training in information security awareness spreads far beyond the Information Technology college courses.

Information security and privacy of students' data are not solely IT issues. Some practitioners (Bogart, 2011) would go so far as to argue that "Information Security is 90% people & process, and 10% technology."

Consequently, training in Information Security needs to be context-aware, i.e., have cyber risks and safe practices components specific to the discipline of student's studies. It may include physical security, ethics, social engineering, social media, eCommerce, laws, and awareness of the impact that a lack of InfoSecurity knowledge may have on other individuals, the university, and the society. Understanding and practicing Cyber Safety and Privacy starts from K-12 schools and should continue through all levels of college education starting from basic skills in IT, cyber security, and privacy. The content and the context of the awareness training will inevitably change over period of time and may depend on the discipline of studies.

A University' curriculum for freshmen in all majors should include topics on online security, privacy, laws, and ethics. Instructors and administrators also need to receive training to help better prepare students for digital age (Alliance, 2011). The goal of such curriculum enhancement is to assure that students are aware and practice safe online and off-line computing and information handling; that they are aware of risks, have knowledge and are able to protect their data at home, on campus, and in cloud computing.

The baseline requirements for an enhanced curriculum should address the following (University of Houston, 2011; Gross, 2011):

1. Recognize computer security risks.
2. Take the appropriate steps to eliminate or decrease those risks.
3. Have a basic knowledge of computer security practices.
4. Take the appropriate steps to secure the university and their own computers.
5. Take advantage of the latest security tools.

The basic principles of Information Security remain the same whether they are applied to corporations or individuals: assurance of confidentiality, integrity, and availability. Building students' capability in these areas will make them better equipped with knowledge and practices to protect themselves and the society from Cyber Security threats.

REFERENCES

Allen, G. (2011). Hitting the Ground Running. *Security, 48*(12), I, 44-46.

Alliance (2011). 2011 National K-12 Study Fact Sheet: The 2011 State of Cyberethics, Cybersafety, and Cybersecurity Curriculum in the U.S. Survey.

StaySafeOnline.org. Retrieved from http://www.staysafeonline.org/search?x=37&y=11&q=study.

Bogart, K. (2011). Information Security Awareness: How to Get Users Asking for More, *White Papers, Management Information Systems.* Eller College of Management, The University of Arizona. December 12, 2011. Retrieved from http://iasec.eller.arizona.edu/docs/whitepepers/IS_awareness.pdf.

Cohon, J. (2009). Academic Role in Securing Cyberspace. *EDUCAUSE Review, 44*(5), 4.

Davidson, M. (2005). Leading by Example: The Case for IT security in Academia. *EDUCAUSE Review*, 40(1), p. 14.

FBI (2005). 2005 FBI Computer Crime Survey. *FBI Publications*. Retrieved from http://mitnicksecurity.com/media/2005%20FBI%20Computer%20Crime%20Survey%20Report.pdf.

Fischer, E. (2005). Creating a National Framework for Cybersecurity: An Analysis of Issues and Options. *CRS Report for Congress.* Retrieved from http://www.fas.org/sgp/crs/natsec/RL32777.pdf.

Gross, G. (2011), Advanced Security Tools Coming Soon. *Computerworld, 45*(12), 4.

Groves, R. (2009). *Survey Methodology*. Wiley Series in Survey Methodology, Edition: 2.

Harris, S. (2013). *All-In-One CISSP*. McGraw-Hill. Sixth edition.

ISC2 (2010). The 2010 State of Cybersecurity from the Federal CISO's Perspective. *An (ISC)^2 Report*. Retrieved from https://www.isc2.org/ciso/Default.aspx.

ITU (2005). A Comparative Analysis of Cyber Security Initiatives Worldwide. *International Telecommunication Union, WSIS Thematic Meeting on CyberSecurity.* Document: CYB/05, 10 June 2005. Retrieved from http://www.itu.int/osg/spu/cybersecurity/docs/Background_Paper_Comparative_Analysis_Cybersecurity_Initiatives_Worldwide.pdf.

Jackson, W. (2012). *Cybersecurity research gets boost in 2013 budget request.* Retrieved from http://gcn.com/articles/2012/02/14/cybersecurity-2013-federal-budget-request.aspx.

Mills, J. (2008). *Privacy: The Lost Right.* Oxford University Press, New York, 2008.

Monash University (2012). Measurement Scales. *Math & Stats.* Faculty of Information Technology. Monash University. Retrieved from http://www.csse.monash.edu.au/~smarkham/resources/scaling.htm.

RedHat (2012). *Issue Severity Classification.* RedHat. Retrieved from https://access.redhat.com/security/updates/classification.

SMB (2011). *New Survey Results Question Actual Cyber Security Preparedness Levels in U.S. SMB's.* Continuity Compliance.org. Retrieved from http://www.continuitycompliance.org/new-survey-results-question-actual-cyber-security-preparedness-levels-in-u-s-smbs.

UC Davis (2008). *Quick Guide to Privacy of Student Records (FERPA).* Office of Student Judicial Affairs. UC Davis. Retrieved from http://sja.ucdavis.edu/files/quickguide.pdf.

University of Houston (2011). CSATS - Computer Security Awareness Training for Students. *Awareness and Training.* University of Houston. Retrieved from http://www.uh.edu/infotech/security/awareness-training/csats.

AUTHOR BIOGRAPHY

Ludwig Slusky is a professor of Information Systems at California State University, Los Angeles (CSULA) and a Certified Computer Information Systems Security Professional (CISSP). His research interests are in cybersecurity and databases. Throughout his career, Dr. Slusky worked as a computer systems consultant for civil engineering, oil, banking, manufacturing, health, and computer industries. Dr.Slusky's intellectual contributions include a book in Database Design Cases and publications in various journals and conference proceedings.

Parviz Partow-Navid has been at California State University, Los Angeles since 1983. Partow-Navid, who is a professor of information systems, currently is serving as Acting Associate Dean of Undergraduate Studies. His papers in the information systems area are published in journals such as The Computers and Operations Research, Journal of Systems Management, Journal of Information Technology Management, and Software Engineering. Dr. Partow-Navid's research interests are in cyber security, intelligent systems, e-commerce, and distance learning.