http://dx.doi.org/10.14236/ewic/HCI2018.117

Towards Comprehensive Information Security Awareness: A Systematic Classification of Concerns among University Students

Ali Farooq
Department of Future Technologies
University of Turku, Finland
alifar@utu.fi

Shamil Alifov
TurkuSec Ry
Turku, Finland
ShamilAlifov@protonmail.com

Seppo Virtanen
Department of Future Technologies
University of Turku, Finland
Seppo.virtanen@utu.fi

Jouni Isoaho
Department of Future Technologies
University of Turku, Finland
Jouni.isoaho@utu.fi

In this paper, we have systematically identified and classified information security concerns (ISCs) of university students into areas where users perceive information security threats. 354 university students were asked to elicit their level of concern on a given set of 74 ISCs using a 7-point scale. Factor analysis (PCA) produced an 11-factor solution, each factor depicting an area of concern. These areas were related to Personal (legal awareness), Social (Sociality), Institutional (Staff member lapses, University networks), Technological (Online social network use, Intrusive service providers, Web browsing and email, Smartphone use, Electronic device use, and Conventional threats), and Non-technological (Cards and wallets security) aspects of student's day-to-day life. The majority of the students (66%) showed concerns related to online social network use, whereas, only 40% of them shown concerns related to sociality. The highest level of concerns was related to service providers, whereas the lowest level of concerns was related to sociality.

Information security, concerns, information security awareness, students, areas of concern, factor analysis, principal component analysis, affinity diagram

1. INTRODUCTION

Like in any other organisation, information security is one of the concerns for the educational institutions (Kerievsky & Bruce, 1976). Information security has been ranked as one of the top areas of concerns for educational institutions in the United States (Ingerman & Yang, 2011). The availability of huge amounts of computing power and open access has attracted the attention of malicious entities towards higher educational institutions (HEIs) (Katz, 2005). HEIs, university, institution and educational institutions have been used in this paper, all referring to institutions imparting post-secondary education (bachelor's level and above). However, HEIs are considered to have poor protection regarding the security of their information assets (Rezgui & Marks, 2008).

A variety of technical (Aurigemma & Panko, 2012) and non-technical measures (Abraham, 2011; Bulgurcu et al., 2009; D'Arcy et al., 2009; Pahnila et al., 2007) have been suggested to safeguard organizational and individual security. Security education, training, and awareness (SETA) programs are suggested as a tool to improve information security awareness of the users (Kim, 2014). ISA has been considered as one of the defences against continuously evolving threat landscape, and a way to mitigate security attacks (Aloul, 2010; Furnell & Clarke, 2012; Siponen & Oinas-Kukkonen, 2007; Tsohou, et al., 2008). ISA enables a user to understand his role in the security process and encourages her/him to take necessary measures for his, as well as his peers, information security (Amankwa et al., 2014; Tsohou et al., 2008). The importance of ISA is similar for a different type of users, be it employees of an organisation (McCormac et al., 2017; Parsons, et al., 2014), or home users(Howe, et al., 2012; Kritzinger & von Solms, 2010), or the students (Kim, 2014; Farooq & Kakakhel, 2013; Kim, 2013).

According to the Concerns-based Adoption Model (CBAM) (Loucks-Horsley, 2010), having a concern is first to step towards change and to learn a new behaviour. If a person is concerned about a phenomenon, s/he will try to get awareness about it

leading to a stage where he will be able to adopt the change or learn the required skill. Keeping in view the importance of ISA, researchers have studied the concept thoroughly, including its antecedents as well the consequences (Jaeger, 2018). However, in most of the available studies, security experts identify an area where ISA is to be assessed and improved, based upon their expert knowledge, and end-users (employees, home-users, students) are involved in assessment phase. Research shows that perceptions of threats play an important role toward (in)action of the end-users that would ensure or endanger information security of users (Milne, et al. 2009). Users have different mental models related to information security threats (Camp, 2009) and resultantly threats are perceived differently. Therefore, we suggest that end-users' concerns be taken into consideration at the time of identifying areas where ISA is to be assessed and improved. If we can understand the users' security concerns, their prevalence and variation, whole ISA process can be improved.

Moreover, the researchers have studied ISA in isolation, that is, within one component or area such password-related behaviour Stanton, et al., 2005), application security in computers (Furnell, et al. 2006) or smartphone security (Mylonas, et al., 2013); while others took a more holist approach where more than one components/areas were used for assessing ISA (Crossler, et al., 2017; Farooq, et al., 2015; Parsons et al., 2014). There is need to identify a set of areas related to the day-to-day life of users where their information security can be jeopardized. Such areas then combined with areas identified by the security experts can provide a comprehensive set of areas where ISA of the users can be improved.

Keeping in view the above gaps, we conducted this study to systematically identify students areas of concerns where they have security concerns. In this study, 74 concerns were rated by 354 university students on a 7-point scale. The concerns were classified into 11 areas using factor analysis which covers five aspects of student's life (personal, social, institutional, non-technological and technological). Further, the prevalence of concerns, level of concerns and variation in the level of concern among different student groups was also examined to understand if the identified areas actually represent students' areas of concerns. Following questions are formulated in this regards:

RQ1: What are the areas where students have information security concerns (Identification of areas)?

RQ2: How are the areas related to students (Connecting concerns with students)?

RQ3: How prevalent are different concerns among the university students within identified areas (Prevalence of concerns)?

RQ4: What is level of concerns among the students within the identified areas? (Level of concern)

Rest of the paper is organised as follow: Section 2 provides narrates the methods and measures used in the study. Section 3 contains the findings and answers to the research questions. Section 4 contains the concluding remarks, followed by a bibliography and the appendix.

2. METHODOLOGY

2.1 Participants, Setting, and Measures

Data on security concerns were collected from students of a Finnish university using an online survey forum, webropol, during 2017. There was no benefit, monetary or otherwise, offered to survey participants. 417 responses were collected in total which were reduced to a usable sample size of 354. The survey took 25-30 minute on an average.

Seventy four concerns were taken from (Farooq et al., 2016), and each was presented with a standard statement "How concerned you are for…" in the questionnaire. A 7-point measurement scale (1: not at all concern to 7: extremely concerned) was used. An option of "I don't know" was also provided. Five items measuring gender, educational level, discipline, previous information security related training (categorical) and age (continuous) were also added. (For detail on concerns consult appendix A.

2.2 Data Analysis

Principle Component Analysis (PCA) was conducted using principal axis factoring with the oblique rotation, as recommended by (Osborne, et al., 2009) in SPSS (v 25,0). Initially, we identified 14 factors using Kaiser criterion (Fabrigar, et al., 1999) (having eigenvalues greater than 1), allowing item loading greater than 0,4, explaining a total variance (TVE) of 69,90%. We repeated the same step by removing items having loadings less than 0,4; no or few item cross-loadings; items; items with cross loading difference more than 0,15 or loading heavily (0,40) on more than one factors were removed; and, items loading on the different components measure different constructs. Haywood cases were removed (item loading greater than 1,0). We also kept in mind the face validity of the factors, that is, similar items should be loaded under one factor, and if not, such items were removed. Once the right factors were reduced after a couple of iterations, we observed that one of the factors contains items each explaining three different concepts. At this point, to reduce the data

loss, we relaxed our criteria of no fewer than three items per factor and divided the factor into three factors explaining three different concepts. In this way, we came up with a solution consisting of 11 reliable and stable factors, explaining 68,87% of the variance. 23 items were dropped (highlighted as *italic* in Annexure) while attaining reliable and stable factors.

3. RESULTS

3.1 Sample Characteristics

Sample characteristics are shown in Table 1:

Table 1: *Sample Characteristics*

Item	Characteristics	%
Gender	Female	54,20
	Male	45,80
Age group	<21	26,60
	21-25	68,40
	>26	5,10
Current Educational Level	Bachelor (UG)	65,00
	Masters (PG)	35,00
Educational Discipline	Economics	34,20
	Education	12,40
	Humanities	2,50
	IT/CS/Engineering	28,80
	Medicine	1,10
	Natural Sciences	19,50
	Social Sciences	1,40
Previous Training	Yes	30,00
	No	70,00

3.2 Identifying Areas of Concern *(RQ1)*

Factors along with item loadings are shown in Table 2. Item loadings cannot be shown as pattern matrix due to the paper template design. For item description, consult the Annexure. To assess the reliability of the factors, we calculated Cronbach's alpha for each factor and found all factors to be above an acceptable level (0,70). Table 2 shows the 11 areas of concerns identified using factor analysis.

Factor 1 (F1) consists of concerns related to online social networks and thus given the title "Online social networks use" [OSN] (α=0,922). Factor 2 (F2) depicts concerns related to lapses by university staff and named "Staff members lapses" [STAFF] (α=0,853). Factor 3 (F3) shows students' lack of awareness towards reading terms & conditions of application and knowing about local cyber laws and termed as "Legal awareness" [LEGAL] (α=0,762). Factor 4 (F4) consists of concerns related to web browsing and emails and named as "Web browsing and email" [B&E] (α=0,909). Factor 5 (F5) consists of concerns that may arise due to interaction with family members, friends, classmates or while working with the class fellows and thus termed "Sociality" [SOC] (α=0,862). Factor 6 (F6) consists of concerns related to conventional threats such as phishing and brute force attack and, thus, named as "Conventional threats" [CTHR] (α=0,817). Factor 7 (F7) depicts the concerns related to university's network and termed as "University networks" [UNET] (α=0,916). Factor 8 (F8) shows concerns that are related to theft or loss of non-technical items, such as cards and wallets, losing which may result in a threat to information security of the students. This factor was named as "Cards and Wallets security" [C&W] (α=0,927). Factor 9 (F9) relates to personal electronic devices (PEDs) and named as "PED Use" [PED] (α=0,822). Factor 10 (F10) consists of concerns that may arise while using smartphones and termed as "Smartphone Use" [SPH] (α=0,901). The Factor 11 (F11) consists of concerns that may arise due to service/application providers and named as "Intrusive Service Providers" [SPRV] (α=0,725). (The abbreviations mentioned after each factor title are used in the Figures and Tables and are mentioned here for better readability)

Table 2: *Factors along with item loadings depicting areas of concern (concern descriptions are in the Appendix)*

Factor	Con-cerns	Load-ings	Factor	Con-cerns	Load-ings
F1 [OSN]	*OSN7*	*0,780*	*F7 [UNET]*	*UCN3*	*0,675*
	OSN6	*0,779*		*UCN4*	*0,672*
	OSN5	*0,763*		*UCN7*	*0,663*
	OSN8	*0,746*		*UCN2*	*0,643*
	OSN9	*0,633*		*UCN6*	*0,627*
F2 [STAFF]	*OC3*	*0,717*		*UCN5*	*0,609*
	OC6	*0,671*		*UCN1*	*0,604*
F3 [LEGAL]	*OC4*	*0,658*		*UCN8*	*0,599*
	OC1	*0,511*		*SIS2*	*0,574*
F4 [B&E]	*WA3*	*0,649*	*F8 [C&W]*	*PB4*	*0,862*
	EM2	*0,648*		*PB3*	*0,849*
	EM1	*0,633*		*PB2*	*0,839*
	WQ4	*0,604*		*PB1*	*0,767*
	WA2	*0,591*	*F9 [PED]*	*PED4*	*0,714*
	WA5	*0,574*		*PED2*	*0,692*
	WA6	*0,564*		*PED3*	*0,674*
F5 [SOC]	*PnI6*	*0,799*	*F10 [SPH]*	*SP4*	*0,752*
	PnI5	*0,776*		*SP6*	*0,7*
	PnI3	*0,745*		*SP5*	*0,677*
	PnI2	*0,743*		*SP7*	*0,623*
	PnI7	*0,728*		*SP3*	*0,584*
	PnI1	*0,68*		*SP8*	*0,537*
F6 [CTHR]	*OSN1*	*0,78*	*F11 [SPRV]*	*OS1*	*0,765*
	PW4	*0,742*		*OS3*	*0,705*
	EM4	*0,68*		*OS2*	*0,654*
	OSN3	*0,512*			

(Kaiser-Meyer-Olkin Measure of Sampling Adequacy: 0.946, Bartlett's Test of Sphericity: 13580.86, df:1275, p<0.001)

3.3 Connecting Concerns with Students *(RQ2)*

To clarify the connection between students and areas of concern, we employed affinity diagramming technique (Grant & Booth, 2009) to group the related areas. An affinity diagram is a tool that is used to organise data (ideas, opinions, issues) into groups based on their natural

relationship. We came up with an affinity diagram consisting of 5 groups covering 11 areas of concern. Each group was given a title and represents one of the day-to-day facets of a student's life. Figure 1 depicts areas of concerns and how they are connected with students' day-to-day life.

3.4 Prevalence and Level of Concerns

To examine prevalence of concerns among the identified areas, we divided the area concern score into three groups, a) absence of concern (point 1 to 4 of 7 point scale), b) presence of concern (point 5 to 6 of 7 point scale), and c) lack of awareness ("I don't know" option). Then, we calculated the percentage of prevalence of concerns within an area. We also employed chi-square test identify the difference in prevalence of concerns. Figure 2 shows the prevalence of concerns was significant differences depicted by '*' with area code in the. In comparison, the highest number of respondents (66%) have concerns related to online social networks (OSN), whereas, the area for which least number of respondents (40%) have concerns was sociality (SOC). Except for SOC, more than half of respondents (at least 54%) have concerns within all the areas.

While the prevalence of concerns show if concerns are present or absent within an area among the students, the level of concern enable us to see how concerns vary among the students. Table 3 shows descriptive for 11 identified areas in descending order of mean scores. The originally coded "I don't know was removed while calculating descriptive statistics. The highest level of concern was found related to intrusive behaviour by service providers such as search string collection by search engines, targeted advertisement, excessive data collection by service providers for marketing purpose and data leakage from the cloud services. The lowest level of concerns was related to sociality. The concerns within this area were mostly related to family members, close friends and peers in the classroom and university. Intrusive Service Providers, Cards and Wallets security, Online Social Networks, Smart Phones and Staff Lapses turned out to be top 5 areas where students have a higher level of concerns.

4. CONCLUDING REMARKS

This paper describes initial findings of an ongoing work on systematic identification of students' concerns about their information security. Data was on security concerns was colleted from 354 university students. Using factor analysis, eleven areas, where students perceive to have information security concerns, were identified. These areas are related to personal, social, institutional, technological and non-technological aspects of students' life. The personal aspect includes legal awareness, the social aspect includes sociality, and the institutional aspect has areas such as university network and staff members lapses. Most of the identified areas (6/11) were related to the technological aspect: online social network use, intrusive service provider, smartphone use, conventional threats, electronic device use and web browsing and email. Cards and wallet security falls into the non-technological aspect of a student's life. Students's concern prevale in most of the areas. In future, we will examine differences in prevelance may arise due to difference in gender, educational background and previous security training.

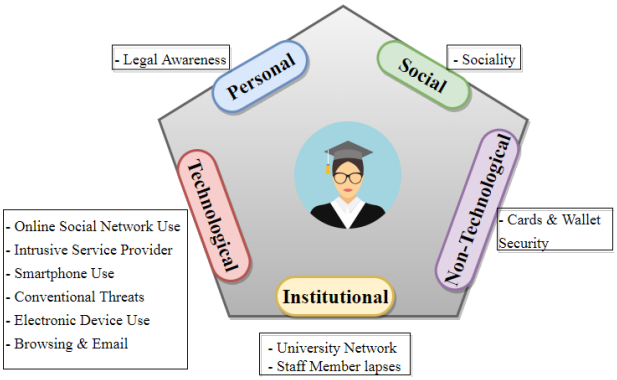

Figure 1: *Areas of concerns and Different Aspects of Student's Life*

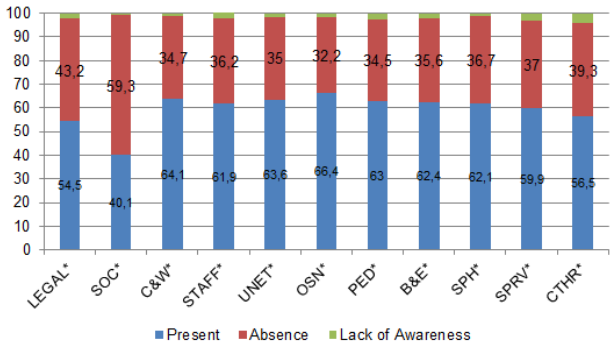

Figure 2: *Prevalence of Concerns within Areas with significant differences (p<0.05)*

Table 3: *Result of Means, Medians, Modes, Standard Deviations for the level of concerns for different areas*

#	Areas	N	Mean	Median	Mode	SD
1	SPRV	343	5,02	5,33	7	1,48
2	C&W	350	5,01	5,50	7	1,95
3	OSN	349	5,00	5,60	7	1,79
4	SPH	350	4,95	5,17	7	1,70
5	STAFF	347	4,93	5,50	7	1,78
6	PED	345	4,83	5,00	7	1,74
7	UNET	349	4,82	5,00	7	1,60
8	CTHR	339	4,76	5,00	7	1,70
9	LEGAL	346	4,75	5,00	7	1,85
10	B&E	347	4,74	4,86	7	1,62
11	SOC	354	3,82	3,83	1	1,76

APPENDIX

List of concerns can be requested from the first author or downloaded from: https://goo.gl/cyo7sm

4. REFERENCES

Abraham, S. (2011). Information Security Behavior: Factors and Research Directions. In *AMCIS 2011*.

Aloul, F. A. (2010). Informa tion Security Awareness in UAE: A survey paper. In *2010 International Conference for Internet Technology and Secured Transactions.* (pp. 1–6). IEEE.

Amankwa, E., Loock, M., & Kritzinger, E. (2014). A conceptual analysis of information security education, information security training and information security awareness definitions. In *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)* (pp. 248–252). IEEE.

Aurigemma, S., & Panko, R. (2012). A Composite Framework for Behavioral Compliance with Information Security Policies. In *45th Hawaii International Conference on System Sciences* (pp. 3248–3257). IEEE.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2009). Roles of information security awareness and perceived fairness in information security policy compliance. In *15th Americas Conference on Information Systems 2009, AMCIS 2009* (Vol. 5, pp. 3269–3277).

Camp, L. J. (2009). Mental models of privacy and security. *IEEE Technology and Society Magazine*, *28*(3), 37–46.

Crossler, R. E., Bélanger, F., & Ormond, D. (2017). The quest for complete security: An empirical analysis of users' multi-layered protection from security threats. *Information Systems Frontiers*, 1–15.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User Awareness of Security Countermeasures and its Impact on Information Systems Misuse: A Deterence Approach. *Information Systems Research*, *20*(1), 79–98.

Fabrigar, L. R., Wegener, D. T., Maccallum, R. C., & Strahan, E. J. (1999). Evaluating the Use of Exploratory Factor Analysis in Psychological Research. *Psychological Methods*, *4*(3), 272–299.

Farooq, A., Isoaho, J. J., Virtanen, S., & Isoaho, J. J. (2015). Information Security Awareness in Educational Institution: An Analysis of Students' Individual Factors. In *Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015* (Vol. 1, pp. 352–359). IEEE.

Farooq, A., & Kakakhel, S. R. U. (2013). Information security awareness: Comparing perceptions and training preferences. In *Conference Proceedings - 2013 2nd National Conference on Information Assurance, NCIA 2013* (pp. 53–57). IEEE Computer Society.

Farooq, A., Kakakhel, S. R. U., Virtanen, S., & Isoaho, J. (2016). A taxonomy of perceived information security and privacy threats among IT security students. In *10th International Conference for Internet Technology and Secured Transactions, ICITST 2015* (pp. 280–286). IEEE.

Furnell, S., & Clarke, N. (2012). Power to the people? The evolving recognition of human aspects of security. *Computers & Security*, *31*(8), 983–988.

Furnell, S. M., Jusoh, A., & Katsabas, D. (2006). The challenges of understanding and using security: A survey of end-users. *Computers & Security*, *25*(1), 27–35.

Grant, M. J., & Booth, A. (2009). A typology of reviews: an analysis of 14 review types and associated methodologies. *Health Information & Libraries Journal*, *26*(2), 91–108.

Howe, A. E., Ray, I., Roberts, M., Urbanska, M., & Byrne, Z. (2012). The Psychology of Security for the Home Computer User. In *2012 IEEE Symposium on Security and Privacy* (pp. 209–223). IEEE.

Ingerman, B. L., & Yang, C. (2011). Top-Ten IT Issues, 2011. *EDUCAUSE Review*, *46*(3), 24.

Jaeger, L. (2018). Information Security Awareness: Literature Review and Integrative Framework. In *51st Hawaii International Conference on System Sciences.*

Katz, F. H. (2005). The Effect of a University Information Security Survey on Instruction Methods in Information Security. In *Proceedings of the 2nd annual conference on Information security curriculum development - InfoSecCD '05* (p. 43). New York, New York, USA: ACM Press.

Kerievsky, B., & Bruce. (1976). Security and Confidentiality in a University Computer Network. *ACM SIGUCCS Newsletter*, *6*(3), 9–11.

Kim, E. B. (2013). Information Security Awareness Status of Business College: Undergraduate Students. *Information Security Journal: A Global Perspective*, *22*(4), 171–179.

Kim, E. B. (2014). Recommendations for information security awareness training for college students. *Information Management & Computer Security*, *22*(1), 115–126.

Kritzinger, E., & von Solms, S. H. (2010). Cyber security for home users: A new way of protection through awareness enforcement. *Computers & Security*, *29*(8), 840–847.

Loucks-Horsley, S. (2010). *Designing professional development for teachers of science and mathematics*. Corwin Press.

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and Information Security Awareness. *Computers in Human Behavior*, *69*, 151–156.

Milne, G. R., Labrecque, L. I., & Cromer, C. (2009). Toward an Understanding of the Online Consumer's Risky Behavior and Protection Practices. *Journal of Consumer Affairs*, *43*(3), 449–473.

Mylonas, A., Kastania, A., & Gritzalis, D. (2013). Delegate the smartphone user? Security awareness in smartphone platforms. *Computers & Security*, *34*, 47–66.

Osborne, Jason W., Costello, A. B. (2009). Best practices in exploratory factor analysis: Four recommendations for getting the most from your analysis. *Pan-Pacific Management Review*, *12*(2), 131–146.

Pahnila, S., Siponen, M., & Mahmood, A. (2007). Employees' Behavior towards IS Security Policy Compliance. In *2007 40th Annual Hawaii International Conference on System Sciences (HICSS'07)* (p. 156b–156b). IEEE.

Parsons, K., McCormac, A., Butavicius, M., Pattinson, M., & Jerram, C. (2014). Determining employee awareness using the Human Aspects of Information Security Questionnaire (HAIS-Q). *Computers & Security*, *42*, 165–176.

Rezgui, Y., & Marks, A. (2008). Information security awareness in higher education: An exploratory study. *Computers & Security*, *27*(7), 241–253.

Siponen, M. T., & Oinas-Kukkonen, H. (2007). A review of information security issues and respective research contributions. *ACM SIGMIS Database*, *38*(1), 60.

Stanton, J. M., Stam, K. R., Mastrangelo, P., & Jolton, J. (2005). Analysis of end user security behaviors. *Computers and Security*, *24*(2), 124–133.

Tsohou, A., Kokolakis, S., Karyda, M., & Kiountouzis, E. (2008). Investigating Information Security Awareness: Research and Practice Gaps. *Information Security Journal: A Global Perspective*, *17*(5–6), 207–227.