A Taxonomy of Perceived Information Security and Privacy Threats among IT Security Students

Ali Farooq*[1], Syed Rameez Ullah Kakakhel[1], Seppo Virtanen[1], Jouni Isoaho[1]
[1]Department of Information Technology, University of Turku, Turku, Finland
{alifar, srukak, Seppo.virtanen, Jouni.isoaho}@utu.fi

Abstract— **The purpose of this study is to explore students' perceived information security and privacy (IS&P) threats and to classify them in a way that helps in analyzing the problem, creating awareness measures and further improving students' IS&P education. Using a qualitative research approach, a group of forty two Master's degree IT students identified seventy five IS&P threats related to them. The identified threats were classified into fourteen categories. Further, using the affinity diagraming technique, the categories were grouped into four domains - Personnel, Devices, Intranet and Internet. In this way, we defined a taxonomy of students' perceived IS&P threats as well as a model that highlights the domains where students consider themselves prone to IS&P threats. The proposed taxonomy and the domain model can be used as a benchmark for designing information security awareness assessment instruments as well as preparing information security awareness programs. The taxonomy can also be used for highlighting areas where students lack information security related knowledge.**

Keywords-component; Information Security, Information Security Awareness, Taxonomy of threats, Threat Landscape, Perceived Threats, Privacy, educational institutions, universities and colleges Introduction (Heading 1)

I. INTRODUCTION

Effective information security (IS) programs should be designed keeping in view the objectives and mission of the organization; and that "understanding the customer's needs must be the first step in establishing an effective information security program" [1]. Organizations invest a significant amount of resources, money and time, in technical measures for their data protection ignoring the involved human element [2]. The diversified attack vectors and threat actors call for measures beyond technical fortification. Literature suggests IS policies, security education, training and information security awareness (ISA) programs as additional measures to strengthen the human factor against cyber threats in the organizations [3, 4, 5]. Aforementioned measures require *customer's needs* assessment to understand an organization's objectives and mission, as well as to measure the present ISA level of the employees (users). In this regard, several studies have addressed IS and ISA in business organizations [6, 7, 8]. At the same time understanding threats is crucial to design countermeasures to mitigate risks [9].

Examining end users' perceived threats can be helpful in understanding customer's needs and in designing a comprehensive ISA assessment and training programs. Information Security and Privacy (IS&P) risks to assets come from IS&P threats and context affect the perceived [10]. Therefore, organizations as a context can influence perceived IS&P risks as well as the perceived threats. So it will not be prudent to consider perceived IS&P risks and threats to one organization directly applicable for an altogether different organization.

Educational institutions, like other organizations, have been hot targets for cybercriminals due to their vast computing power and open access [11]. Educause Review [12] has ranked IS as one of the top areas of concern for educational institutions in the United States for last several years. However, very few IS&P related studies are focused on educational institutions in general and students in particular. For example, [13] is focused on employees' ISA in educational institutions, [14] is about information security strategies and [15] talks about adoption of IS in higher education institutions. Among the very few studies that target student's ISA in the educational institutions context, the focus is either on comparing preferences of students towards sources of accumulating ISA and training [16], providing guidelines and recommendations for ISA training for college students [17] or studying the relationship of different students' individual factors with ISA [18]. However, we could not find a study that identifies and examines students' perceived IS&P related threats in the context of educational institutions. Business organizations have commercial goals and their personnel structure consists of two human entities – employee and employer/management, leaving out clients and suppliers. On the other hand, the goal of educational Institutions (universities, colleges, and schools) is to impart education and learning to a third human entity called students. The applicability of rules and regulations is different for students as compared to typical employer-employee structured organizations. Thus, the perceived threats to commercial organizations cannot be considered applicable to educational institutions due to difference of contexts.

Taking into account the abovementioned disparity, we conducted this exploratory study to identify, examine and classify students' perceived IS&P threats. For this purpose, as a first step, we used a qualitative research approach to find answers to the question "what are students' perceived IS&P threats in the context of an educational institution?" The whole research process was rooted in Grounded Theory, wherein a model is built upon data collection from the entities directly related to the phenomenon under study. Through an open ended question, data was collected from 42 master degree students from the information technology (IT) discipline. After examining the answers, 75 perceived threats were identified

from the responses of the students. These were then classified into 14 categories using content analysis. The categories are Personal Belongings, Proximity/Interaction, Smart Phones, Other Personal Electronic Devices (PEDs), Network Administration, Privacy Policy Issues, University Communication Network, Students' Information Systems, Email, Online Social Networks, Online Services, Web Access, Passwords and Others. Further, using the affinity diagraming technique, these categories were grouped into four domains - Personal, Device, University Intranet and the Internet. In this way, we not only examined the students' perceived IS&P threats but also proposed the Student's Perceived Threats Domains (SPTD) model.

The rest of the paper is organized as follows. Section II provides theoretical background and Section III explains the research approach used for this study. Section IV details the results and discussion, and in section V we give concluding remarks as well as outline future directions that will be built upon the model proposed in this paper.

II. THEORETICAL BACKGROUND

A. *Information Security Awareness*

The perusal of literature reveals that there is IS researchers define and understand ISA differently as a concept. Some consider it only as seeking the attention of individuals towards IS [19] while others suggest that ensuring compliance is also included in addition to directing the individuals [20]. Maybe this vagueness is inherited from the word "awareness" that can be interpreted into different meanings depending upon the interpreter. [6] suggests that the possible ambiguity of the ISA definition is because it is a socially constructed concept.

Since one of our future objectives is designing an ISA assessment tool, like [16,21], we consider ISA as the combination of knowledge and behavior. The knowledge of facts, processes and concepts is one of the three important cognitive skills for an effective learning process. The other two are the ability to apply the knowledge and the ability to reason [22]. So, if a person has knowledge of IS&P threats, s/he can apply that knowledge to avoid the risks.

B. *Classification of threats*

The classification of specimens into taxonomy provides an approximation of reality that gives better understanding of the phenomenon under study [23]. Grouping and classifying information system threats has been used in the past for understanding the threats and providing countermeasures for them. Researchers use a different basis for classification that in turn gives different perspectives. For example, [24] categorizes information system's threats based upon type of assets such as hardware, software, data, network, physical, personnel and administrative; [25] proposes a model based upon four dimensions, sources, perpetrators, intent and consequences; [26] propose a list containing leading information system threats into data processing errors, network breakdowns, software flaws, loss of key personnel and so on. [27] provides a list of studies wherein information system threats have been grouped and classified. Moreover, there are studies wherein classification has been done based upon either attack techniques [28, 29] or threat impacts [30]. [31] proposes a hybrid classification model wherein both attack techniques and threat impacts are taken into consideration. The aforementioned classifications and models provide us with the understanding of threats related to information systems and provide a guideline for security managers and professionals to design countermeasures.

However, we were unable to find a study wherein students' perceived threats have been examined, classified and modeled. Moreover, keeping in view our future objective of designing a comprehensive ISA assessment tools for educational institutes, the aforementioned classifications lack in providing a viewpoint that is crucial for designing an ISA assessment tool as well as for providing education and training of end users (students).

III. RESEARCH APPROACH

This section describes the overall research approach of the study, including the research overview, the method, the materials and the procedure.

A. *Purpose of the study and the research process*

The purpose of this exploratory study is to identify and examine students' perceived IS&P threat landscape to develop a systematic presentation that could help in analyzing the problem, creating awareness measures and further improving the students' IS&P education. In doing so, we have (a) identified students' perceived IS&P threats with their help (b) classified them into categories; and (c) grouped them into domains. Fig. 1 shows the objective of the study in an abstract form. This abstract form suggests that one or more threats can be classified into categories which then may constitute domains. One category can cover one or more threats, similarly one domain can cover more than one category.

The research process of this study consists of three steps and is shown in Fig. 2. In the first step, we identified the perceived threats with the help of a group of students. The experts (researchers in IS) then classified the identified threats into categories and further into groups. Validation of the resulting taxonomy and/or domain model is beyond the scope of this paper and will be carried out later during the second phase of our research with the help of a bigger sample of (1) students with different educational and cultural backgrounds, and (2) IS professionals, researchers and teachers.

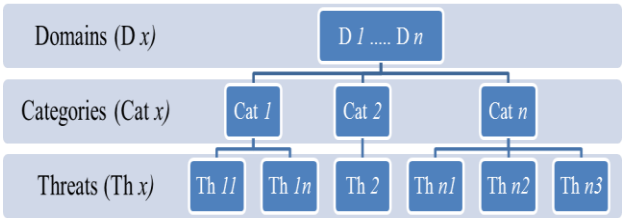

Figure 1: Objective of study in abstract form

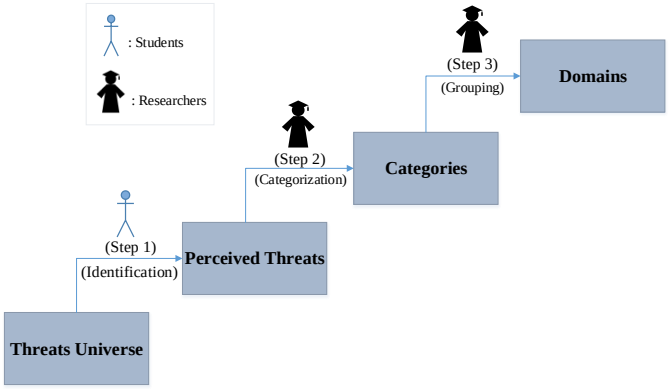

Figure 2: Research process of the study

B. Method

For data collection, we adapted the focus group approach wherein *n*=42 (male=39, female=3) Master's degree IT security students from our university participated. The gender imbalance in our sample was by chance as the majority of participating students in the class were male at time of data collection. We used IT students as the target group for two reasons. (1) IS professionals might be experts in their domain, however, their perceived IS&P threats cannot be the same as the ones perceived by the students, (2) a recent study [16] shows that IT students have higher IS knowledge as well as higher perceived ISA in comparison to students from other disciplines. So it was deemed appropriate to use IT students as a preliminary target audience to collect data from. However, it would be interesting to conduct a similar study for students from other disciplines. Since the aim of this study was to explore the students' perceived IS&P threats and to classify them, we are not focusing on detailed demographic information except for gender and age. The age group of the student expert group was 20-32. Detailed background and demographic information will be taken into consideration at the time of model validation. All the group members had prior knowledge of information security and privacy concepts.

C. Materials and procedure

As mentioned in Fig. 2, the whole process consisted of three steps. In Step 1, using an open ended question, the participants were asked to list their perceived IS&P threats as a university student. This question was given to them as a part of a course assignment on human element in information security. The response was obligatory as it was part of an assignment to be graded for course credits, in addition to being used as data for this study. Therefore, the obligation in this case did not affect the students' responses but would compel them to think harder. The respondents were not asked to provide any justification for their responses Our focus was only on "what" and not on "why" and "how" at the time of the study. We believe introducing "why" in an exploratory study like ours can lead to desultory discussions by the participants. The data was collected during March 2015.

In Step 2, the responses from the participants were examined by two experts (researchers of IS) using content analysis separately. Following rules were adopted during the examination:

1. The threats will be examined with respect to the function and/or service being at risk. For example, one of the students mentioned that "*...Also some unintentional personal details can be sent to wrong email if for example automatic signature in use.*" This particular threat was related to emails.
2. The threats related to same function and/or service will be put into one category.
3. The threat will be put into the relevant category based upon cause but not the effect. For example, the participants mentioned that weak passwords for payment services are a threat to students' IS&P. So the cause is the weak password and not the payment service and hence this threat was categorized into category "Passwords" and not into "Online Services".

Once the content analysis had been done by the experts separately, they sat together and cross-checked the extracted threats and the categories. After discussions and deliberations, seventy five identified perceived threats were put into fourteen categories. Each category was constructed keeping in view the principles of classification [23]. The categories were given meaningful names based upon the function and/or service. In this way we developed a taxonomy of students' perceived IS&P threats. Fig. 3 presents the taxonomy, showing the categories as well the threats.

In Step 3, the categories were examined by four experts and grouped them into the domains using the affinity diagram technique [32]. Again the discussion took place and four mutually agreed domains were finalized. These domains were named Personal, Devices, University Intranet and Internet.

IV. Results and Discussion

The examination of data collected from the group of students reveals that they mentioned seventy five different IS&P threats. In this study, the focus was to identify the perceived threats and not to prioritize them. Furthermore, we did not inquire about the consequences of these threats and possible countermeasures against them. Identified threats were then classified into categories using content analysis. Most of the identified threats were related to security and privacy. However, there were a few related to surveillance and they were not considered for this study.

The participants showed their concerns regarding a wide range of threats, from online social networks (OSNs) to the university's communication network and from smartphones to their wallets. Some of them also tried to elaborate their perceived IS&P threats by providing context and places where particularly they find themselves at risk. For example, a male participant finds a cafeteria a place where someone can see his banking card's pin code through shoulder surfing. Another example is a female student who believes working in a diverse group for class assignment using OSN can result in privacy issues as well as identity theft for her.

A. *Categories*

The perceived IS&P threats are classified into following fourteen categories:

1) *Personal Belongings*

The group identified non-electronic items such as the student ID card, banking cards (debit and credit cards) and the wallet as important items in terms of IS&P. Nowadays, students have a multipurpose student ID enabling them to access different facilities within the university, such as printing services and the library as well as using it as a payment card in the cafeteria. The theft/loss of such cards can deprive the students from these services and if fallen in the wrong hands, the information stored in the cards can be misused. The group also mentioned that their wallets contain important items that can compromise their privacy in case they fall in the hands of a malicious party. Losing a banking card can result in financial loss to the students. Therefore, theft/loss of the aforementioned personal belongings was considered a privacy threat by the students.

2) *Proximity/Interaction*

The participants also mentioned IS&P threats that were related to their personal interactions and locations within the university. For example, someone peeping onto your laptop's screen and stealing your passwords for university login or even for online banking credentials; learning banking card details (card holder name, card number and the customer verification code (cvc)) while standing in queue for payment in university cafeteria; someone looking at your laptop screen and trying to know what you are doing or even copying your assignment; connecting your laptop to a multimedia projector in a classroom and accidentally revealing your password on the big screen. In addition to that, the participants also mentioned possible threats that could come from connections such as friends and boy/girlfriend. For example, lending your device (mobile, laptop etc.) to your friend is a potential privacy threat as s/he may explore your device – accessing SMS messages, emails or even pictures; your boy/girlfriend gets to know your passwords and upon breakup, may access your account(s), change password(s) or even blackmail you. One of the female participants considered making a group on a social media platform and working together for class assignments as potential privacy risk.

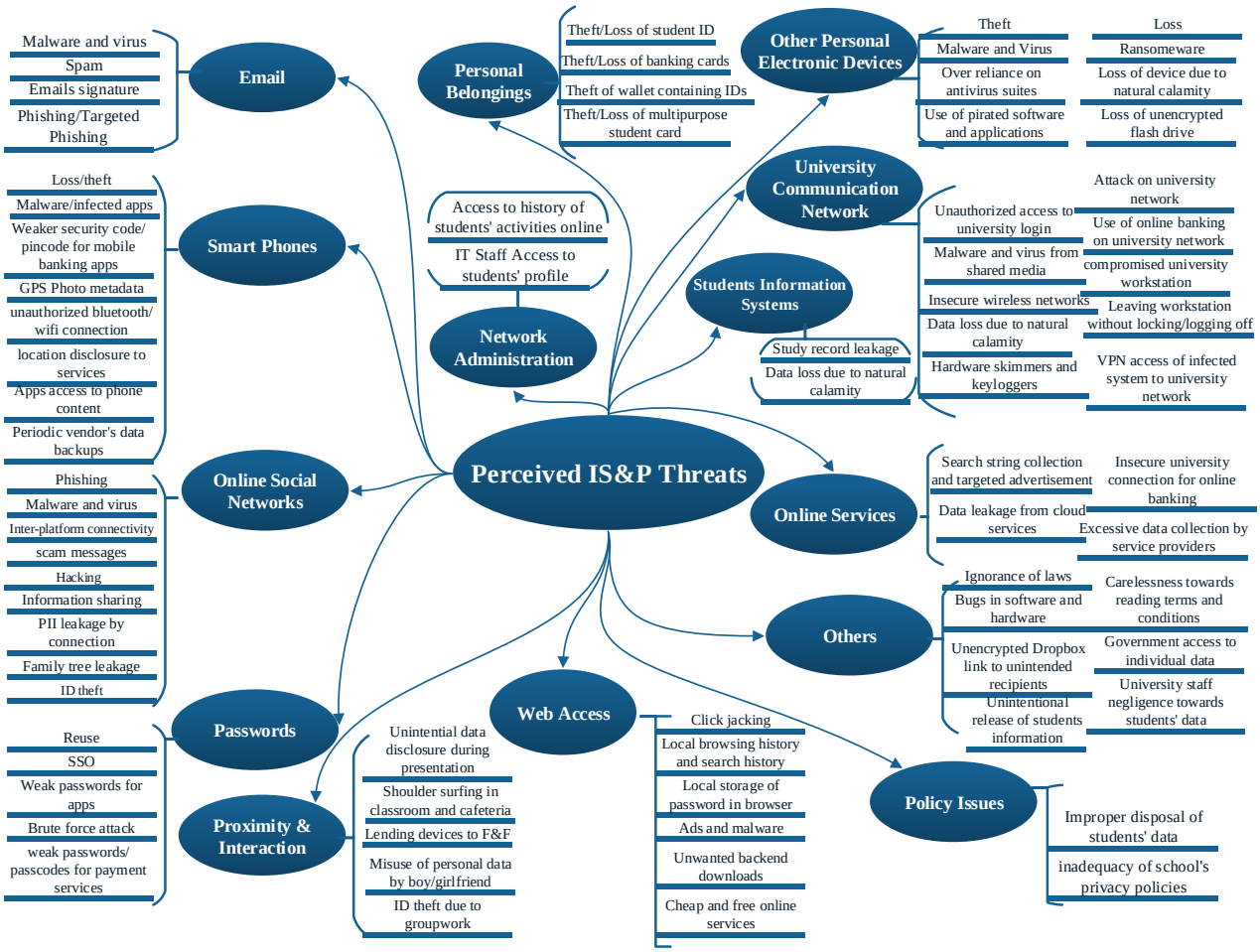

Figure 3: Taxonomy of students' perceived threats

3) Smart Phones

A number of reports have shown smart phones as one of the biggest IS threat to an organization [33, 34]. Perusal of the group's responses revealed that students were also concerned about IS&P threats related to smart phones. The students identified more threats regarding smartphones as compared to IS&P threats to any other categories stated in this paper. Theft, loss, malware and infected apps were considered IS threats. Furthermore, weak security codes for mobile banking (four digits) were also considered a security threat. Students also considered unauthorized Bluetooth or WiFi connections as a security threat. In terms of privacy, location disclosure to apps, GPS photo metadata, an app's access to phone contents and periodic backups by app vendors were considered as threats.

4) Other Personal Electronic Devices

All the threats related to the laptops, computers, mobile phones, tablets and flash drives were put into the category of personal electronic devices (PEDs). The threats particular to smartphones have already been discussed above. The participants considered malware and viruses, use of pirated software, over-reliance on anti-virus suits and ransomware as IS threats related to PEDs. The loss/theft of any of the aforementioned devices, the theft/loss of an unencrypted flash drive, and device losses due to a natural calamity such as fire, earthquake or an accident were among other identified threats.

5) Network Administration

According to the participants of the study, authorized and unauthorized access by IT staff to students' profile information, browser's browsing history and activity log on university network are IS&P threat to the students. It seems to be a tradeoff between effective network management and students' perceived IS&P threats.

6) Privacy Policy Issues

Participants of the study also identified policy related issues that can be possible IS&P threats for the students, for example, inadequacy of privacy policies at university. They also considered the school's information retention policies, wherein students' information (personal and educational) is kept for a certain number of years before disposal, as a potential privacy threat to the students.

7) University Communication Network

The participants mentioned a number of perceived threats related to university communication networks, for example, malware and virus infections from the university's shared storage media, an insecure wireless network, a compromised workstation on the university network, hardware skimmers and keyloggers. Using an online banking service on the university network was considered a potential financial risk. Students log into a university workstation in the library, and forgetting to log off was mentioned by several participants as well. Access to the university network via VPN from an infected machine was also perceived as a threat.

8) Students' Information Systems

The participants mentioned a couple of IS&P threats related to students' information systems. The participants believed that an attack on the university network can result in leakage of students' records which is a privacy threat to them. Furthermore, any unauthorized access to students' records in the university can expose the students to security and privacy threats. Loss of devices containing students' information due to natural calamities was also considered as IS&P threat.

9) Email

Email is one of the most powerful tools used for communication these days and at the same time it invites many malicious intent entities to exploit its power to reach. Like other users, students are prone to a wide range of security threats while using email. The participants considered malware, viruses, spam, phishing/targeted phishing as IS threats, whereas, disclosing email signature to an unintended recipient was considered a privacy threat.

10) Online Social Networks

A study [35] suggests that the use of OSNs among students is on the rise. The participants identified a number of security and privacy threats related to OSNs. Among security threats, they identified phishing, malware, viruses, scam messages, hacking and inter-platform connectivity as threats to students' information security. Excessive information sharing by themselves, personal identifiable information (PII) shared by their connections and the leakage of family tree information was considered as threats to their privacy in OSNs. One of the participants mentioned that his lack of social media presence makes impersonation easier for a malicious intent entity and since he does not have any OSN accounts, someone can make a fake account and impersonate him.

11) Online Services

According to [17], the use of online services is on the rise amongst students due to online resources such as MOOCs and digital libraries. Students use search engines and cloud services for both learning and recreational purposes. The participants of this study considered data leakage from cloud services, search string collection by search engines and targeted advertising, data collection by service providers (websites and web services) and insecure connections while using online banking or user authentication as perceived IS&P threats.

12) Web Access

Students access internet for different educational and recreational purposes. Therefore, it was interesting to see what IS&P threats students perceived in the web. We found that participants are concerned of threats related to browsers, malware and unwanted download. The participants considered the browsing history and the search history saved in the browsers as a threat to their security and privacy. Furthermore, they also mentioned local storage of passwords (remember my password option) as a perceived IS&P threat. Click-jacking, Ads that install malware and unwanted application downloads were the other perceived IS&P threats by the participants.

They also perceived cheap and free online services as a threat because it leads to potential spamming.

13) Passwords

Passwords are a cost effective and easily implemented method for authentication yet poor password management practices lead to security issues [36]. The participants perceived that students can have a number of IS&P threats due to poor management of passwords, for example, the reuse of a password, the use of weak passwords and passcodes for payment services, brute force attacks against passwords and single sign-on (SSO) were considered as threats to students' IS&P.

14) Others

The participants of the study also identified IS&P threats that could not be placed in any of the aforementioned categories. Moreover, since this study was exploratory and it was expected that more threats would be identified at the time of validation, we kept such threats in the 'Others' category for the time being. Examples of such threats are ignorance of students resulting in possible malicious action that is punishable under certain laws, carelessness towards reading terms and conditions of the apps and services, government access to a private company's data on an individual, negligence of university staff that results in privacy issues for the students, unintentional release of students' records that are searchable through search engines, threats caused because of bugs in the software and hardware and sharing links to unencrypted files in Dropbox to unintended recipients by mistake.

B. *Students' Perceived Threats Domains*

Once the categories were classified, we then grouped the identified categories into four domains. These domains were named Personal, Devices, Intranet (University Intranet) and Internet and are shown in Fig. 4. This grouping was done using the affinity diagraming technique [32]**.** It was also found that the categories Passwords and Others cover more than one domain and they are hence placed accordingly.

With help of threats, categories and domains we were able to identify the students' perceived threat domains (Fig. 4) which can be used to understand the possible IS&P threats to students. It shows that students use different devices such as laptops, university workstations, smart phones and other smart devices such as tablets to login to the university intranet which further has connectivity to the Internet. Students' identified threats within domains of personal, devices and intranet can be termed as on-campus threats and the threats that lie in the Internet can be termed as off-campus threats. We named the above mentioned model the Students' Perceived Threats Domains (SPTD) Model. We will validate this model with help of students with diverse educational and cultural backgrounds in our next study.

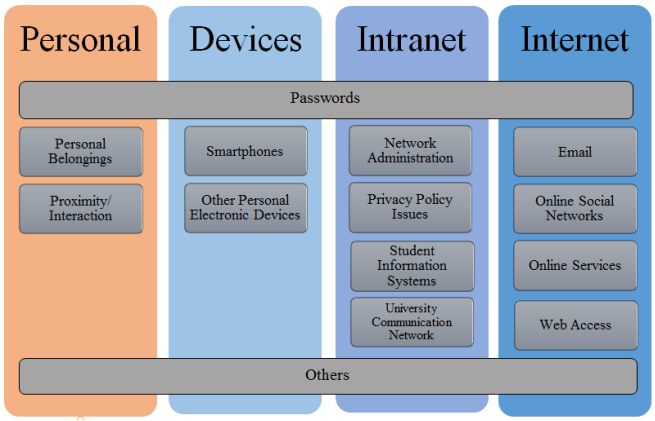

Figure 4: Students' perceived threats domains model

V. Conclusion And Future Directions

In this paper, we have identified and examined different information security and privacy (IS&P) threats perceived by a group of university IT security students. Using a bottom up approach, data was collected from a group of 42 Master's degree IT Security students using open ended question. Content analysis and the affinity diagram technique were employed to identify, classify and group students' perceived threats into categories and domains. The resultant taxonomy provides a student's viewpoint of threats and the domains where such threats exist. The taxonomy presented in this paper shows that the group of IT Security students have a holistic understanding of IS&P threats beyond devices and networks. The taxonomy also shows that most of the perceived IS&P threats are related to the Internet. On the other side, there are threats that can prove risky to students due to their interactions and proximity. Our taxonomy is different from previous similar studies wherein taxonomies of information systems' threats were presented as a view of security professionals and employees only.

The Students' Perceived Threats Domains (SPTD) Model elaborates the landscape where students can be prone to different IS&P threats. The taxonomy and the model presented in this paper can be used as a benchmark for designing information security awareness programs. The list of threats used in this taxonomy and the domain model is not exhaustive, rather both taxonomy and domain model provide space to accommodate future threats related to students.

This paper is based upon initial findings from a study that gives a glimpse of students' awareness of different threats. The model presented in this paper requires validation from a bigger sample of students from diverse educational and cultural backgrounds. It would be interesting to see how students from different cultures fit into this model. Our group was male dominant by chance and hence a gender balance inquiry is also of interest. The domain model can be used to study perceived threats at junior level as well.

REFERENCES

[1] T. R. Peltier, "Implementing an Information Security Awareness Program." *Information Systems Security*, vol. 14, pp. 37-49, 2005.

[2] L. Connolly and M. Lang, "Information Systems Security: The Role of Cultural Aspects in Organizational Settings," *Information Systems Security*, 2013.

[3] S. Pahnila, M. Siponen and A. Mahmood, "Which factors explain employees' adherence to information security policies? An empirical study," PACIS 2007 Proceedings, pp. 73, 2007.

[4] S. Abraham, "Information security behavior: factors and research directions", Proceedings of the American Conference on Information Systems, Detroit, Paper 462, 2011.

[5] D'Arcy and A. Hovav, "Does one size fit all? Examining the differential effects of IS security countermeasures," Journal of Busisness Ethics, vol. 89, pp. 59-71, 2009.

[6] A. Tsohou, S. Kokolakis, M. Karyda and E. Kiountouzis, "Investigating information security awareness: research and practice gaps," Information Security Journal: A Global Perspective, vol. 17, pp. 207-227, 2008.

[7] B. Lebek, J. Uffen, M. H. Breitner, M. Neumann and B. Hohler, "Employees' information security awareness and behavior: A literature review," in System Sciences (HICSS), 2013 46th Hawaii International Conference on, 2013, pp. 2978-2987.

[8] L. Cheng, Y. Li, W. Li, E. Holm and Q. Zhai, "Understanding the violation of IS security policy in organizations: An integrated model based on social control and deterrence theory," *Comput. Secur.*, vol. 39, pp. 447-459, 2013.

[9] Q. Yeh and A. J. Chang, "Threats and countermeasures for information system security: A cross-industry study," *Information & Management*, vol. 44, pp. 480-491, 2007.

[10] B Fischhoff. "Risk Perception and Communication" in Oxford Textbook of Public Health, 5th edition. R Detels, R Beaglehole, MA Lansang, and M Gulliford, Ed. Oxford: Oxford University Press, Sage, 2009, pp 940-952.

[11] F. H. Katz, "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, 2005, pp. 43-48.

[12] B.L. Ingerman, and C. Yang,. (2011). "Top 10 IT issues 2011",Educause Review, May/June, pp. 26-40.

[13] H. Chan and S. Mubarak, "Significance of Information Security Awareness in the Higher Education Sector," *International Journal of Computer Applications*, vol. 60, 2012.

[14] R. D. Butler, An Examination of Issues Surrounding Information Security in California Colleges. PhD Dissertation, Northcentral University, 2013.

[15] H. Kam and P. Katerattanakul, "Information security in higher education: A neo-institutional perspective," Journal of Information Privacy and Security, vol. 10, pp. 28-43, 2014.

[16] A. Farooq and S. R. Ullah Kakakhel, "Information security awareness: Comparing perceptions and training preferences," in *Information Assurance (NCIA), 2013 2nd National Conference on*, 2013, pp. 53-57.

[17] E. B. Kim, "Recommendations for information security awareness training for college students," Information Management & Computer Security, vol. 22, pp. 115-126, 2014.

[18] A. Farooq, J. Isoaho, S. Virtanen, J. Isoaho, "Information security awareness in Educational Institution: An analysis of students' individual factors," in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2015 IEEE 14th International Conference on*, Helsinki, Finland, 2015, in press.

[19] M. Wilson and J. Hash, "Building an information technology security awareness and training program," NIST Special Publication, vol. 800, pp. 50, 2003.

[20] M. Siponen, "Five dimensions of information security awareness," Computers and Society, vol. 31, pp. 24-29, 2001.

[21] H. A. Kruger, L. Drevin, and T. Steyn, "A vocabulary test to assess information security awareness". *Information Management & Computer Security*,*18*(5), 316-327,2010.

[22] I. V. Mullis, M. O. Martin and P. Foy, IEA's TIMSS 2003 International Report on Achievement in the Mathematics Cognitive Domains: Findings from a Developmental Project. ERIC, 2005.

[23] U. Lindqvist and E. Jonsson, "How to systematically classify computer security intrusions," in *Security and Privacy, 1997. Proceedings., 1997 Ieee Symposium on*, 1997, pp. 154-163.

[24] D. Icove, K. Seger and W. VonStorch, *Computer Crime: A Crimefighter's Handbook.* O'Reilly & Associates Sebastopol, CA, 1995

[25] K. D. Loch, H. H. Carr and M. E. Warkentin, "Threats to information systems: today's reality, yesterday's understanding," *Mis Quarterly*, pp. 173-186, 1992.

[26] K. J. Fitzgerald, "Information security baselines," *Information Management & Computer Security*, vol. 3, pp. 8-12, 1995.

[27] Q. Yeh and A. J. Chang, "Threats and countermeasures for information system security: A cross-industry study," *Information & Management*, vol. 44, pp. 480-491, 2007.

[28] L. Ruf, A. Thorn, T. Christen, B. Gruber, R. Portmann. "Threat modeling in security architecture - the nature of threats." Internet: https://www.isss.ch/fileadmin/publ/agsa/ISSS-AG-Security-Architecture__Threat-Modeling_Lukas-Ruf.pdf, 2008 [Access Date: May 25, 2015]

[29] M. Alhabeeb, A. Almuhaideb, P. D. Le and B. Srinivasan, "Information security threats classification pyramid," in *Advanced Information Networking and Applications Workshops (WAINA), 2010 IEEE 24th International Conference on*, 2010, pp. 208-213.

[30] J. Meier, A. Mackman, M. Dunner, S. Vasireddy, R. Escamilla and A. Murukan, *Improving Web Application Security: Threats and Countermeasures.* Microsoft Redmond, WA, 2003.

[31] M. Jouini, L. B. A. Rabai and A. B. Aissa, "Classification of security threats in information systems," *Procedia Computer Science*, vol. 32, pp. 489-496, 2014.

[32] H. Beyer and K. Holtzblatt, *Contextual Design: Defining Customer-Centered Systems.* Elsevier, 1997.

[33] Ponemon, "2013 state of the endpoint,", Ponemon Institute LLC, Traverse City, Michigan, 2012.

[34] D. J. Kuss and M. D. Griffiths, "Online social networking and addiction—a review of the psychological literature," *International Journal of Environmental Research and Public Health*, vol. 8, pp. 3528-3552, 2011.

[35] D. J. Kuss and M. D. Griffiths, "Online social networking and addiction—a review of the psychological literature," *International Journal of Environmental Research and Public Health*, vol. 8, pp. 3528-3552, 2011.

[36] F. Mwagwabi, T. McGill and M. Dixon, "Improving compliance with password guidelines: How user perceptions of passwords and security threats affect compliance with guidelines," in *System Sciences (HICSS), 2014 47th Hawaii International Conference on*, 2014, pp. 3188-3197.