Cyber Security Awareness of Engineering Students: A Qualitative Analysis on Computer & Mechatronic Departments

Hasan TINMAZ and Mehmet Ali BARIŞKAN

***Abstract*—Furnishing university students with the necessary Information and Communication Technologies (ICTs) has been an indispensable instructional activity for the last decade. When it comes to the engineers, who are the technological stakeholders and decision makers, these instructional activities become even more important. This article discusses how computer (n=6) and mechatronic (n=6) engineering students in their fourth year perceive cyber security phenomenon after finishing a cyber security course. With a qualitative interviewing technique and analysis, it was revealed that students were satisfied with the course in terms of cognitive and affective acquisitions. As a result, students seemed not highly aware of adverse effects of lacking cyber security precautions. Moreover, even though mechatronic engineering students are in ICTs field, they seemed to have less concerns and interest related to cyber security. The study enlightens how cyber security courses should be instructionally designed and implemented.**

***Index Terms*— Cyber Security, Higher Education, Security Teaching, Security Awareness**

I. Introduction

INFORMATION and Communication Technologies (ICTs) are central elements of our daily lives. ICTs (especially the Internet) have brought many advantages to humanity while creating new concerns such as security in macro (countrywide national security) and micro (personal use) levels. It was predicted that 70% of world population would be using the Internet in 2015 [1] which also means that 70% of the entire world population might face these concerns in any second. Cyber security is one of the major concerns of this century. According Merriam Webster dictionary, cyber security means "measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack" [2]. In that sense, cybersecurity covers different tools, processes and actions deliberately developed for shielding computers, software, data and networks from attack, illegal access and damage. Generally, when the ICTs stakeholders talk about security, they highly refer to cyber security. As being that significant in personal and professional lives, knowing and taking actions about cyber security are obligatory for all ICT users.

According to Norton, as being a computer security firm, the cost of security investment was $100 billion in 2012 [1]. This cost increased $400 billion in 2014 where it was also estimated that cybercrime costs reflecting on the global economy would increase that cost every single year [3]. Moreover, in parallel to the increase in number of mobile devices and smart device users are generally unaware that they are under threat from these devices. As a result, the investments, need of cyber security knowledge and awareness toward cyber security are getting higher and higher. For instance; while downloading and/or installing apps from unknown providers, users make themselves open to attacks which deactivate security procedures setup by manufacturers [4].

A well known cyber security company, Cyren, released "2015 Cyberthreat Yearbook Report" in early March 2015, which compared threats with year of 2014. According to the report use of malicious software increased by 50%, "phishing" e-mails 233%, malware affecting Android-based mobile systems increased by 61%, in comparison to 2014 [5]. Moreover, Turkish Data Security Association [Bilgi Güvenliği Derneği] added that cyber security threats are not only resulting from technological issues, but also from human aspects requiring awareness toward cyber security related issues [6].

As a consequence of its significance, cyber security and its training are getting widespread both in education and business sectors. It is expected that engineers who are the planners, adapters, users and multipliers of ICTs, play an important role regarding with cyber security issues. Therefore, engineers should attend cyber security courses to develop themselves in both knowledge and awareness level. In these courses, the difficult part is to make students understand how important cyber security is so that it reflects their overall perception of cyber security in knowledge and implementation levels. Affective domain of cyber security (aka psychological approach of students on cyber security) is the most important

Assist. Prof. Dr. Hasan TINMAZ. Istanbul Gelisim University, Faculty of Engineering and Architecture, Department of Computer Engineering. Cihangir mah. Şehit Jandarma Komando Er Hakan Öner Sk. No:1 Avcılar / İstanbul / Turkey (corresponding author to provide phone: +90 5324159940; fax: +90 2124227401; e-mail: htinmaz@gelisim.edu.tr).

Res. Assist. Mehmet Ali BARIŞKAN. Istanbul Gelisim University, Faculty of Engineering and Architecture, Department of Computer Engineering. Cihangir mah. Şehit Jandarma Komando Er Hakan Öner Sk. No:1 Avcılar / İstanbul / Turkey (e-mail: mabariskan@gelisim.edu.tr).

part of it, as they will decide for security procedure in their prospective jobs.

Literature also recommends that cyber security teaching/learning is important not only for engineering students but also for non-engineering students such as psychology and economics [7]. While social media tools (especially, Facebook, Instagram and Twitter) are getting more users who are predominantly from the youngster and youth, cyber security gains are more important for students. Therefore, cyber security awareness must be built into all people's minds [8].

To sum up, awareness of cyber security issues is an initial and vital step for taking precautions against cybercrime. Therefore, this study focuses on computer and mechatronic engineering students' awareness issues regarding with the cyber security after they fulfilled the cyber security course in their faculty.

II. METHOD

A. Research Context

The "TSD411 Cyber Security" elective course was delivered in the "2014-2015 Fall Semester" for computer (n=17) and mechatronic (n=20) departments at a faculty of engineering and architecture at a private university for the senior (fourth year) students (total 37 students). The researchers collected qualitative data via interviews with purposeful sampling at the end of the semester, after the students learnt their overall grades from the course.

B. Research Methods & Analysis

This is a descriptive case study concentrating on revealing perceptions of university students on cyber security as being one of the most important concerns for current ICT world. The students were prospective computer or mechatronic engineers who will work in a key position for giving decisions on ICT work and who took a cyber security course just before this study. A qualitative method was used during the data collection, to obtain comprehensive information. By purposeful sampling technique (which is common in qualitative research [9]), six students from each department were selected for the study (35% of entire computer engineering students, 30% of entire mechatronic engineering students, 33% of entire students registered to course). Students were asked about their course grade; AA (n=1), BB (n=3), CB (n=2), CC (n=2), DC (n=1), and FF (n=2). According to student course grade distribution, it seems that sample represents the class population.

The researchers organized an interview schedule with the help of literature and their professional experiences. After scrutiny from their colleagues and Turkish language experts, the final draft was piloted on a student who was excluded from results of this study. The final version of the interview schedule was applied to the selected students who were informed that their grades would not be affected by their answers. Moreover, none of the researchers were the instructor or any relationship with the course. Therefore, the students were assumed to provide information with less pressure. Interviews were conducted individually at the researchers' office on an appointment based plan.

The data was collected by means of semi-structured interviews with the researchers. The interviews were transcribed and coded. Then, the transcriptions were analyzed by means of content analysis. The researchers conducted an analysis of single transcriptions to create a set of categories and subcategories. Themes derived from each participant's responses were shared and discussed between the researchers.

III. RESULTS

A. Change in knowledge

The first questions were about to reveal how students perceive change in their knowledge on CS (Cyber Security) after they had finished a course on CS. From Table 1, it seems that course did not change their CS knowledge much.

TABLE I
CHANGE IN KNOWLEDGE

Computer Engineering	n	Mechatronic Engineering	n	Total	n
Basic to Intermediate	3	Zero to Zero	1	Zero to Zero	1
Zero to Basic	2	Zero to Basic	3	Zero to Basic	5
Basic to Basic	1	Zero to Intermediate	1	Zero to Intermediate	1
		Basic to Basic	1	Basic to Basic	2
				Basic to Intermediate	3

B. General evaluation of the Cyber Security course

The students were asked evaluate CS course. Nearly all students did not want to make a general comment on the course. 1 student remarked that it was an essential course for his professional development. The students were asked the difficulty level of the course. Table 2 shows that students perceived CS course as a difficult one.

TABLE II
COURSE DIFFICULTY LEVEL

Computer Engineering	n	Mechatronic Engineering	n	Total	n
No Comment	1	Easy	2	No Comment	1
Hard	3	Hard	2	Easy	2
Moderate	1	Very Hard	2	Moderate	1
				Hard	5
				Very Hard	2

Afterwards, the students pointed the underlying reasons of this difficulty. It seems that students had problems with lack of preliminary knowledge, lecturer, and lack of motivation (Table 3).

TABLE III
REASONS OF DIFFICULTIES

Computer Engineering	n	Mechatronic Engineering	n	Total	n
No Comment	2	Not necessary	1	No Comment	2
Introductory topics	1	Requirement of prerequisite knowledge	1	Introductory topics	1
Lecturer could not transfer the knowledge	1	Lecturer's communication skills should be better	1	Lecturer could not transfer the knowledge	1
Lecturer was not dominant in the course	1	Requirement of preparation before the course	1	Lecturer was not dominant in the course	1
Similar with other lessons	1	Students' willingness	1	Similar with other lessons	1
		Use of many terms in English	1	Not necessary	1
				Requirement of prerequisite knowledge	1
				Lecturer's communication skills should be better	1
				Requirement of preparation before the course	1
				Students' willingness	1
				Use of many terms in English	1

C. Necessity of Cyber Security course

When the necessity of having such a course was asked, computer-engineering students strongly agreed whereas mechatronic students had suspicious thoughts on the issue (Table 4).

TABLE IV
NECESSITY OF COURSE

Computer Engineering	n	Mechatronic Engineering	n	Total	n
Yes	4	Yes	2	Yes	6
Absolutely	2	No	2	No	2
		No Comment	1	Absolutely	2
		A little	1	A little	1
				No Comment	1

Furthermore, students were asked about why they feel such a necessity of attending such a course. Some students argued that using a computer or being computer engineering cannot be realized without CS awareness. Mechatronic engineering students did not feel such a necessity to join a course on CS (Table 5).

TABLE V
REASONS OF NECESSITY

Computer Engineering	n	Mechatronic Engineering	n	Total	n
Computer security is in all areas of life	1	No Comment	4	Computer security is in all areas of life	1
Necessary	1	Not Necessary	1	Necessary	1
Cannot think Computer Engineering without security	1	It is a necessity to store personal information safely	1	Cannot think Computer Engineering without security	1
No Comment	3			No Comment	7
				Not Necessary	1
				It is a necessity to store personal information safely	1

Five computer engineering students declared that the CS course must be mandatory where only 1 computer-engineering student noted that CS course should stay as an elective course as it used to be. On the other hand, the situation is totally opposite for mechatronic engineering students where 5 students support elective course idea and 1 only agreed to have CS course as a mandatory in department curriculum.

D. Learning about Cyber Security

Students were questioned to what extent they believe that they learned fundamentals of CS via this course. Unfortunately, half of students did not believe that they had furnished themselves with basics of CS (Table 6).

TABLE VI
KNOWLEDGE LEVEL AT THE END OF COURSE

Computer Engineering	n	Mechatronic Engineering	n	Total	n
Not Really	1	Very Little	1	Very Little	1
No	2	Not completely	1	A little	1
Basics, yes	3	Basics, yes	2	No	2
A little	1	Yes	2	Not Really	1
				Not completely	1
				Basics, yes	4
				Yes	2

For detailed information, students were asked to unfold their reasons for not-comprehending the fundamentals. Most students did not want to make any comment on that issue. Nonetheless, some students noted problems regarding to

technological problems, disliking the course and necessity of having extracurricular study on CS (Table 7).

TABLE VII
REASONS OF THIS KNOWLEDGE LEVELS

Computer Engineering	n	Mechatronic Engineering	n	Total	n
No Comment	5	No Comment	2	No Comment	6
Software & Hardware Problems	1	Course apathy	1	Course apathy	1
		Students required to make additional research & self-development	2	Software & Hardware Problems	1
				Students required to make additional research & self-development	2

Furthermore, the students were asked if their expected topics in CS course were fulfilled or not. Most of the students pointed that many topics they expected to be covered in the CS course were presented during the semester (Table 8).

TABLE VIII
EXPECTED TOPICS FULFILLMENT

Computer Engineering	n	Mechatronic Engineering	n	Total	n
Yes	3	Yes	3	Yes	6
Not Completely	2	Nearly all of them	1	Nearly all of them	1
Not very much	1	Generally	1	Generally	1
		No Comment	1	Not Completely	2
				Not very much	1
				No Comment	1

The students explained why they thought that their expectations in relation to CS course topics were not fulfilled. Students were complaining about departmental differences and pointless topics within the course (Table 9).

TABLE IX
REASONS OF EXPECTED TOPICS FULFILLMENT

Computer Engineering	n	Mechatronic Engineering	n	Total	n
No Comment	4	No Comment	3	No Comment	7
Requires too much research beforehand	1	It is not correct to offer this course to Mechatronic Engineering Department	1	It is not correct to offer this course to Mechatronic Engineering Department	1
Too much unrelated subjects	1	Lecturer helped enough	1	Requires too much research beforehand	1
		More than enough	1	Too much unrelated subjects	1
				More than enough	1
				Lecturer helped enough	1

As a follow-up question, students listed the topics that they wanted to see within CS course. Only one student added that "attacks" should be in CS course curriculum whereas 11 students did not have any comment.

E. Teaching about Cyber Security

The students stated whether or not the CS course should be taught as theory or as implementation based on instruction. Eight of the students (five computer engineering and three mechatronic engineering) remarked that CS course should be implementation based. Four students (one computer engineering and three mechatronic engineering) emphasized that CS course should be both theory and implementation based together in balance.

Additionally, students added their comments on what an implementation based CS course should include. Students want to apply attack and counter attack simulation based on software (Table 10).

TABLE X
PROSPECTIVE TOPICS STUDENTS WANT TO SEE IN THE COURSE

Computer Engineering	n	Mechatronic Engineering	n	Total	n
Attack examples	3	Attack examples	3	Attack examples	6
Security organization against an attack	1	Attack & counter attack programs	3	Attack & counter attack programs	3
Maintaining a Firewall	1			Security organization against an attack	1
Simulative attacks	1			Maintaining a Firewall	1
				Simulative attacks	1

Moreover, the students made comments on instructional materials used in CS course. Less than half of the students were satisfied with the instructional materials used (Table 11).

TABLE XI
LEVEL OF MATERIALS SATISFACTION

Computer Engineering	n	Mechatronic Engineering	n	Total	n
No Comment	1	No Comment	1	No Comment	2
No	3	No	1	No	4
Not Bad	1	Yes	4	Not Bad	1
Yes	1			Yes	5

Students mostly complained about lack of implementation sessions in a computer lab and the language of the materials, which was mostly in English. Similarly, students adversely expressed their attitudes towards the instructor and the course which affected their standpoint toward instructional materials (Table 12).

TABLE XII
REASONS OF MATERIAL SATISFACTION

Computer Engineering	n	Mechatronic Engineering	n	Total	n
Computer Labs had problems including administration rights	3	Computer Labs had problems including administration rights	1	Computer Labs had problems including administration rights	4
Materials were mostly in English (must be Turkish)	2	Materials were mostly in English (must be Turkish)	1	Materials were mostly in English (must be Turkish)	3
Lecturer could not use materials properly	1	I liked the exercises	2	I liked the exercises	2
Not much documents	1	Apathy toward the course	1	Not much documents	1
				Lecturer could not use materials properly	1
				Apathy toward the course	1

In addition to the instructional materials, the students reflected on "assessment criteria" of the CS course. Initially, they did not want to make any comments, although they were already graded at the end of the semester. Some students doubted the exam procedures and instructor's objectivity (Table 13).

TABLE XIII
ASSESSMENT CRITERIA

Computer Engineering	n	Mechatronic Engineering	n	Total	n
No Comment	4	No Comment	3	No Comment	8
I doubt about the quality of exams	1	Students were affecting instructor's grades.	1	I doubt about the quality of exams	1
Assessment criteria were not equal for every student	1	Very Good	1	Assessment criteria were not equal for every student	1
		Correct at both teaching procedure & assessment.	1	Students were affecting instructor's grades.	1
				Very Good	1
				Correct at both teaching procedure & assessment.	1

Students were asked to assume the role of instructor and to tell what kind of assessment activities they would realize in the CS course. Even though minority of the students still would like to have a paper-based exam, the majority notes that they would apply computers based exams in the CS course (Table 14).

TABLE XIV
HOW STUDENTS WOULD DO ASSESSMENTS

Computer Engineering	n	Mechatronic Engineering	n	Total	n
I would care how much students learned from this course than exam results	1	I would grade students based on lab activities	2	I would grade students based on lab activities	2
Mainly, I would make exams in multiple choice formats	1	No Exam at all	2	No Exam at all	2
I would make application based activities and grade them, and additionally I would make an exam	1	No Comment	3	I would care how much students learned from this course than exam results	1
I would give better grades who finalize the activities/attacks first	1			Mainly, I would make exams in multiple choice formats	1
Paper based exam	1			I would make application based activities and grade them, and additionally I would make an exam	1
No Comment	1			I would give better grades who finalize the activities/attacks first	1
				Paper based exam	1
				No Comment	4

The students stated their opinions on how to offer such a course, if they were the course instructor. This is one of the questions that students shared many different instructional ideas (Table 15).

TABLE XV
HOW WOULD STUDENTS OFFER THE LESSON

Computer Engineering	n	Mechatronic Engineering	n	Total	n
Firstly, I would give fundamental terms	2	Same as the professor we got the course	2	Firstly, I would give fundamental terms	2
First theory and then application / implementation	1	More theory	1	I'd divide class into sections	2
Firstly, I would measure the level of students	1	First theory and then application / implementation	1	Same as the professor we got the course	2
I would show them how to attack & defense	1	I never want to deliver this course	1	First theory and then application/implementation	1

I would show them how to install & use the related software	1	I'd divide class to sections	1	Firstly, I would measure the level of students	1
I would select one type attack & focus only on that one	1			I would show them how to attack & defense	1
I'd divide class into sections	1			I would show them how to install & use the related software	1
I'd give research subjects to students	1			I would select one type attack & focus only on that one	1
				More theory	1
				I never want to deliver this course	1
				I'd learn myself first and then offer	1

Lastly, the students (n=10) pointed that universities could establish departments within a faculty or vocational school just focusing on cyber security.

IV. CONCLUSION AND RECOMMENDATIONS

This study reflects on how prospective engineers, who will be the technology stakeholders, perceive cyber security concepts and how a cyber security course could contribute to that perception change. Computer and mechatronic departments were deliberately selected to show that security is an essential element for their work. The results showed that mechatronic students underestimate importance of cyber security by calling it "not an interest for their future work". The cyber security course was pointed as a "not beneficial or not interesting course" for their departmental curriculum. Therefore, there needs to be an awareness movement for mechatronic departments which is directly a part ICTs. Additionally, the cyber security course should have a different section for them emphasizing overtly related cases or examples from implementation of mechatronic engineering. Computer engineering students gave the impression that they had realized the importance of the cyber security for their personal (especially on social media) and professional lives by even highlighting that a computer engineer cannot survive without cyber security knowledge in his/her life.

The results showed that students do not feel comfortable about their cyber security knowledge as a result of lack of attack/counterattack based implementations. It was strongly highlighted that cyber security courses must have more implementation than theory which would be realized in computer labs than regular classes. Moreover, the students noted that cyber security knowledge evaluation must also stem from real case applications, not paper based exams.

Students urged that learning or applying cyber security, students must bring prerequisite knowledge to the class. They even added that the instructors should check that prerequisite knowledge at the beginning of the semester. Filling the gap with what the students should know at the beginning of the semester will increase the motivation and willingness toward the cyber security topics.

Students complained about the course materials, since they are dominantly in English. Therefore, academicians or implementers of cyber security must create more instructional materials (including books and lecture notes) in Turkish.

This study includes small sample of students contributed and qualitative as a method. Qualitative method based studies frequently investigate the research problem in-depth. Therefore, the study results might not generalize to other cases. Based on these findings, future research should be conducted either with a quantitative or mixed research method approaches.

REFERENCES

[1] K. W. Brenda, "The role of psychology in enhancing cybersecurity" *Cyberpsychology, Behavior, And Social Networking*, vol. 17, no.3, pp. 131-132, 2014.

[2] Merriam Webster Dictionary. (2015, August 10). [Online]. Available: http://www.merriam-webster.com/dictionary/cybersecurity

[3] D. Zureich and W. Graebe, "Cybersecurity: The continuing evolution of insurance and ethics" *Defense Counsel J*., vol. 82, no.2, pp. 192-198, April 2015.

[4] J. Imgraben, A.Engelbrecht and K. R. Choo, "Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users", *Behaviour & Information Technology*, vol. 33, no. 12, pp. 1347-1360, June 2014.

[5] Cyren, Inc. 2015 Cyber threat Yearbook., (2015, August 10). [Online]. Available: https://www.cyren.com/tl_files/downloads/CYREN_2015_CyberThreat_Yearbook.pdf

[6] Turkish Data Security Association [Bilgi Güvenliği Derneği]. "Cyber Security Report: First Quarter, 2015". (2015, August 10). [Online]. Available: http://www.bilgiguvenligi.org.tr

[7] J. Cano, R. Hernández, and S. Ros "Bringing an engineering lab into social sciences: didactic approach and an experiential evaluation", *IEEE Communications Magazine*, vol. 52, no. 12, pp. 101-107, December 2014.

[8] B. Simpson and M. Murphy, "Cyber-privacy or cyber-surveillance? Legal responses to fear in cyberspace", *Journal Information and Communications Technology Law*, vol. 23, no.3, pp. 189-191, October 2014.

[9] M.Q. Patton, *Qualitative Evaluation and Research Methods*, Newbury Park, CA: Sage, 1990.

Dr. Hasan Tınmaz, Assist. Prof. received his bachelor's degree from the Department of Computer Education, Faculty of Education, from Middle East Technical University in 2001. He completed his M.Sc. degree in Curriculum and Instruction Program, from the Department of Educational Sciences at METU (2004). He received his Ph.D. from Computer Education and Instructional Technology at METU (2011). He is now is an assistant professor, in the Faculty of Engineering and Architecture, Department of Computer Engineering, at Istanbul Gelisim University. His research focuses on Web 2.0/Web 3.0 technologies, social media, instructional design, and human & computer interaction.

Mehmet Ali Barışkan, Res. Assist. received his bachelor's degree from the Department of Computer Engineering in English, Faculty of Engineering and Architecture, Istanbul Aydin University in 2013. He is currently a graduate student in the Computer Engineering Master Program at the Science Institute of Istanbul University. He is also a research assistant in the Computer Engineering Department, in the Faculty of Engineering and Architecture, Istanbul Gelisim University. His research focuses on computer security, cyber security, data recovery and reverse engineering.