Assessing the level of cybersecurity knowledge of Computer Science and Applied Automation undergraduates

RALUCA DOVLEAC
Department of Management and Industrial Engineering
University of Petrosani
No. 20 Street, Petrosani, Hunedoara
ROMANIA

Abstract: The importance and role of cybersecurity awareness is more pressing than ever in today's modern world and therefore, this concern gave voice to a number of studies evaluating the level of preparedness of individuals and professionals regarding cybersecurity aspects. Furthermore, the number of open positions on the job market in the field of cybersecurity highlight the topicality of the subject. In this paper, the author analyzed the level of knowledge that last year Computer Science and Applied Automation undergraduate students possess and also examined current practices around the world regarding cybersecurity education with the role of understanding the implications of cybersecurity education and proposing a set of measures and activities that can be applied to facilitate the educational process in the field of cybersecurity.

Key-Words: cybersecurity, knowledge, computer science, information technology, information system

Received: August 5, 2021. Revised: March 18, 2022. Accepted: April 22, 2022. Published: June 7, 2022.

1 Introduction

Cybersecurity has continued to be an important area of interest in the past couple of years, more so as an increasing number of companies are turning more to technology and the digitalized environment surrounding their business eco system.

The lack of cybersecurity professionals has been consistent during this time and furthermore, although companies' efforts in term of ensuring cybersecurity have increased, it had been proven time and time again that the weakest link in the cybersecurity chain remains the human factor. Globally, we are witnessing efforts made by professional organizations, government institutions and educational institutions to reach a middle ground and identify the best solutions regarding cybersecurity training and knowledge acquisition.

The present study has been conducted with the purpose of assessing the level of cybersecurity knowledge for last year students – given how they will be entering the job market soon, and to evaluate whether the introduction of a cybersecurity discipline in their degree curriculum would be relevant.

2 Problem Formulation

For a couple of years, the cybersecurity job market has been lacking professionals and furthermore research has shown that even those who are hired in different sectors of activity are at the end of the day the biggest threat to the company's cybersecurity.

Recent trends to combat this phenomenon have focused on developing training materials and a curriculum for educational institutions so that newly hired employees can enter the job market with a decent amount of cybersecurity knowledge.

With this in mind, the author looked to identify the level of cybersecurity knowledge and skills of the last year students at the Computer Science and Applied Automation degrees at the University of Petrosani, and to obtain their perspective regarding the utility of introducing a cybersecurity discipline in their degree curriculum since at the current time, they do not benefit from such training.

2.1 Literature review

The term cybersecurity can be used to express multiple aspects of security in the cyber space such as: preventive actions meant to detect and outsmart potential intruders [1]; prevention of damage or restoration to computers, systems and data [2]; the process or set of activities that protect information and communication systems from modification, unauthorized access or exploitation [3]; a state of being protected against the criminal and/or unauthorized use of electronic data or the set of measures taken to achieve that state [4].

Cybersecurity has become an increasingly important topic in recent years, part of the reason

being the increased number of cybercrimes taking place in the United States [5] (814 cases reported in 2012, 1095 cases reported in 2013 and an increase in 2020 due to the COVID-19 pandemic) [3] [6]. An increased number of attacks have been noted in the past in the health care industry [7] but a recent report by IBM in which top industries affected by cybercrimes were analyzed and categorized based on the attack volume in the year 2020, revealed that the Finance and Insurance industry was the most affected, followed by Manufacturing, Energy, Retail, Professional Services, Government, Healthcare, Media, Transportation and Education [8].

Furthermore, the effect of cyberattacks and their impact on small businesses have also been noted with an estimate of 44-50% of small businesses being the victim of cyberattacks [9] [10] [11]. The costs of recovery from cyberattacks have been estimated to average $38,00 (in direct costs related to down time, external services, unpursued business opportunities and so on) and up tup $8,000 (in indirect costs such as preventive measures focused upon staff, the system and training) [9].

As for the reason that lead to cyberattacks in small businesses, a study conducted by the National Cyber Security Alliance and Symantec on 1000 SME's with less than 250 employees highlighted that 90% of companies don't benefit from having a technology focused IT manager, 68% don't provide any form of cybersecurity training for their employees and 83% don't even have basic cybersecurity practices implemented such as automatic systems to require employees to periodically change passwords [9], even though the latter has been noted as an important aspect of a secure behavior with usage of weak passwords and /or the same password across multiple accounts linked to cybersecurity breaches [12].

Cybersecurity educations aims to help users of technology be aware of the threats they are exposed to [13] [3] and to give them the necessary set of skills and tools that would enable them to overcome these threats.

The efforts of organizations, education institutions and government institution have become more intense in the last couple of years and therefore as a result we can witness the first cybersecurity master programs in top universities across the world [14], professional societies such as ACM and IEEE becoming more involved in defining university curriculum [15], the growing number of conferences on the topic of cybersecurity [16] [17], a number of frameworks for cybersecurity, developed both by governmental institutions [18] [19], as well as practitioners and researchers [20] [21] [22] [23] and even competitions on cybersecurity such as DoD Cyber Crime Center, Digital Forensics Challenge and the NetWars competition being held [5].

2.1.1 Methodology

For the theoretical part of the paper, the author conducted a literature review based on the research available in major indexing databases (such as WoS, Scopus) as well as frequently used and easily accessible databases (Google Scholar). The search parameters used were: 1. research articles, systematic literature reviews, original papers, and review articles that talked about the 2. topic of "cybersecurity", "cybersecurity education", "cyberthreats", "cybersecurity frameworks", "cybersecurity knowledge" as well as different combinations of these keywords, within the following 3. time interval: 2012 – 2022. All of the articles selected for the literature review were checked for relevancy and additional bibliographical sources recommended in the first batch of articles were reviewed as well.

For the practical part of the paper, in order to assess the overall level of cybersecurity knowledge in Computer Science and Applied Automation undergraduates of the University of Petrosani, Romania, the author conducted a study based on a survey constructed by Raineri and Fudge [9], with minor modifications in order to suit the particularities of the students at the University of Petrosani.

The survey consisted of 13 content questions, 12 of which asked the participants about their knowledge of specific cybersecurity topics as well as the means by which they procured that knowledge (whether they had to study by themselves or they learned the information by partaking in a mandatory and/or optional courses at the university where they were doing their studies) and a question asking participants whether they think it would be useful to add a cybersecurity course (whether it is optional or mandatory) in the curriculum. The sample consisted of all the last year students at the Computer Science (32 students) and Applied Automation (36 students) bachelor studies programs at the University of Petrosani, totaling 68 participants for the survey.

The author chose to survey the last year students of these programs since they were the most probable to get hired soon after graduating, becoming therefore part of the new wave of employees on the market and therefore, it is useful to see what skills and capabilities in terms of cybersecurity they

possess. From the total number or participants surveyed (through the help of a survey created in Google Forms and distributed via email) only 29 participants responded, meaning 42.64% of all participants.

3 Results

The results of the questionnaire revealed that overall more than half of the participants either didn't have any knowledge regarding cybersecurity practices or obtained this knowledge through individual study.

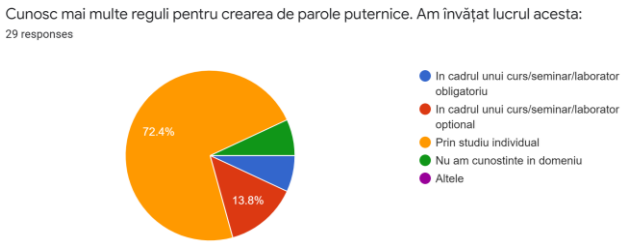

Fig.1 Question no.1 – Passwords

The first statement *"I know multiple guidelines for making strong passwords. I learned this:"* presented in Figure 1 revealed that 72.4% of participants learned how to create strong passwords through individual study, while 13.8% said that they've learned this through the help of an optional course taken at the university.

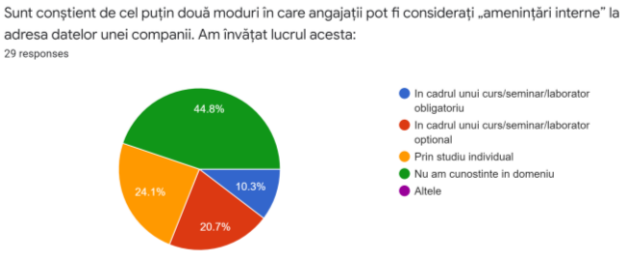

Fig.2 Question no.2 – Employee threats

The second statement *"I am aware of at least two ways employees can be considered "inside threats" to my company's data and/or proprietary secrets. I learned this:"* presented in Figure 2 showed that 44.8% of participants didn't have any sort of knowledge in the field, 24.1% learned of this through individual study, 20.7% learned this through an optional course taken at the university and 10.3% learned this through a mandatory course taken at the university.

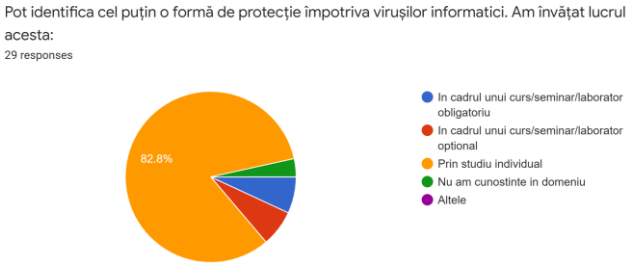

Fig.3 Question no.3 – Viruses

The third statement *"I can identify at least one safeguard against computer viruses. I learned this:"* presented in Figure 3 revealed that the vast majority of participants – 82.8% learned about computer viruses and protection against them through individual study.

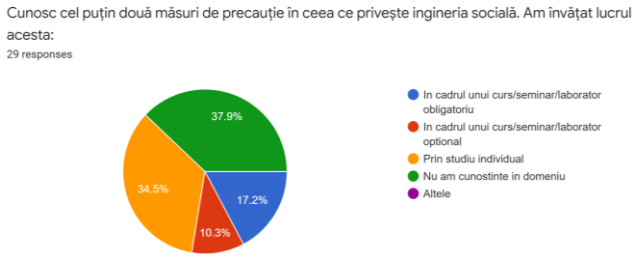

Fig.4 Question no.4 – Social engineering

The results of the fourth statement *"I understand at least two precautions regarding social engineering. I learned this:"* presented in Figure 4 show that 37.9% of participants don't have any knowledge regarding this issue while 34.5% learned about the issue through individual study.

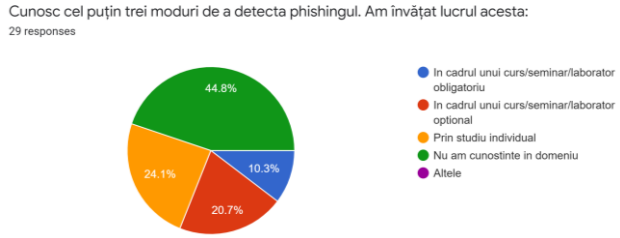

Fig.5 Question no.5 – Phishing

The results of the fifth statement *"I know at least three ways to spot phishing. I learned this:"* presented in Figure 5 show that almost half of participants (44.8%) don't have any knowledge regarding this issue while 24.1% learned about the issue through individual study.

Fig.6 Question no.6 – BYOD practices

More than half of the participants (65.5%) have no knowledge regarding the risk of Bring Your Own Device (BYOD) practices as shown in the statement presented in Figure 6*"I am aware of two or more employee BYOD security concerns. I learned this:"*

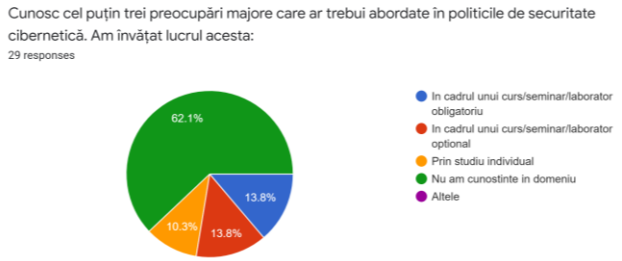

Fig.7 Question no.7 – Cybersecurity policies

More than half (62.1%) of participants have no knowledge regarding cybersecurity policies as it can be observed in the statement presented in Figure 7 of *"I know at least three major concerns that should be addressed in Cyber Security policies. I learned this:"*

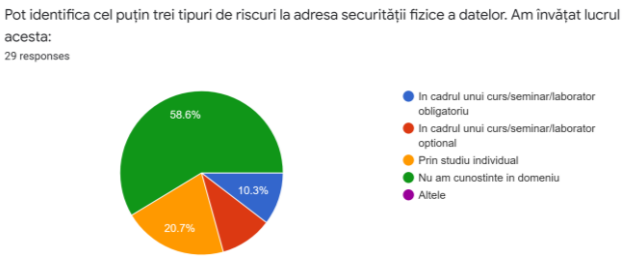

Fig.8 Question no.8 – Physical security of data

The same aspect can be observed in Figure 8 presenting the eight statement of the survey *"I can identify at least three kinds of risks to the physical security of data. I learned this:"* where it can be noted that more than half of participants have no knowledge regarding the physical security of data.

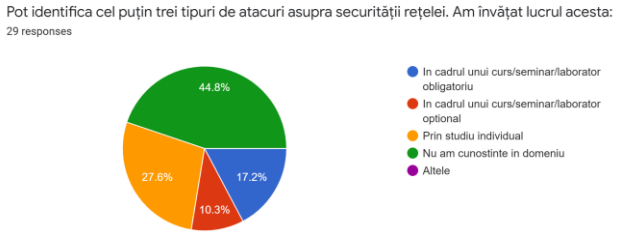

Fig.9 Question no.9 – Network attacks

Almost half of participants (44.8%) have no knowledge regarding network attacks while 27.6% report learning about the topic through individual study as it can be observed in the statement presented in Figure 9 *"I can identify at least three kinds of network security attacks. I learned this:"*

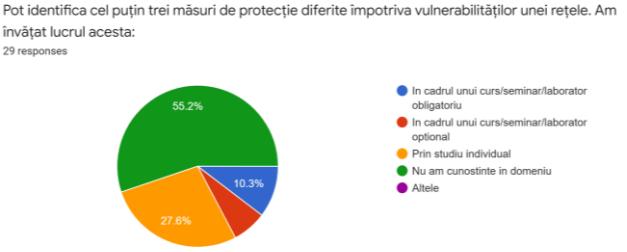

Fig.10 Question no.10 – Network vulnerabilities

More than half of participants (55.2%) reported that they have no knowledge regarding safety methods used for network protection as it can be observed from the statement *"I can identify at least three different safeguards against network vulnerabilities. I learned this:"* presented in Figure 10.

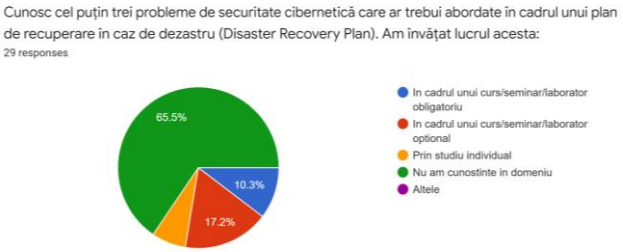

Fig.11 Question no.11 – Disaster Recovery Plans

The results of the eleventh statement *"I know at least three cyber security concerns in that should be addressed in a Disaster Recovery Plan. I learned this:"* presented in Figure 11 show that more than half of participants (65.5%) don't have any knowledge regarding this issue.

The twelfth question of the survey asked the participants to use adjectives in order to describe their perceived level of cybersecurity knowledge. The results are as follows: "limited knowledge" – 5 responses, "decent knowledge" – 3, "sufficient knowledge" – 1.

The last question of the survey presented in results of the fourth statement *"I consider the introduction of a cybersecurity discipline in the curriculum as:"* presented in Figure 12 shows that all respondents considered the introduction of a cybersecurity discipline in the curriculum necessary with an overwhelming number of respondents (72.4%) saying it would be useful for the discipline to be a part of the mandatory classes taken for the degree and the remaining 27.6% saying that it would be useful for the discipline to be an optional one.

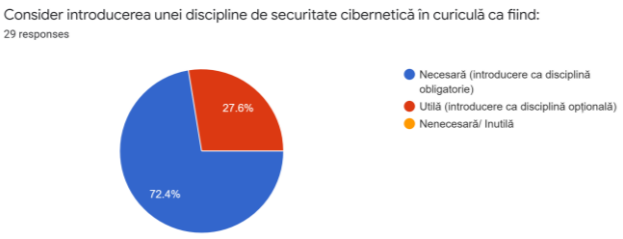

Fig.12 Question no.12 – Cybersecurity in the curriculum

4 Conclusion

The survey revealed that more than half of the participants (from a total of 29 participants) possessed very basic information regarding

cybersecurity and for the vast majority of them, this knowledge has been obtained through individual study rather than a formal training.

The participants of the study were undergraduates in the last year of study, and most of them expressed their desire to get hired upon graduation therefore they will enter the job market with a deficit of knowledge regarding cybersecurity adding to the total of employees on the job market that are underprepared in the field.

Previous studies have shown that cybersecurity training done during the degree studies can be beneficial and furthermore, all of the participants in the study considered that it would be useful to add a cybersecurity discipline in the curriculum.

References:

[1] R. A. Kemmerer, "Cybersecurity," pp. 1-11, 2003.

[2] C. W. Dukes, Committee on National Security Systems, National Security Agency, MD, 2015.

[3] E. Amankwa, "Relevance of Cybersecurity Education at Pedagogy Levels in Schools," *Journal of Information Security*, pp. 233-249, 2021.

[4] Oxford University Press, "Lexico," [Online]. Available: https://www.lexico.com/definition/Cybersecurity. [Accessed 23 05 2022].

[5] R. S. Cheung, J. P. Cohen, H. Z. Lo and F. Elia, "Challenge Based Learning in Cybersecurity Education," 2011.

[6] S. Monteith, M. Bauer, M. Alda, J. Geddes, P. C. Whybrow and T. Glenn, "Increasing Cybercrime since the Pandemic: Concerns for Psychiatry," Current Psychiatry Reports, vol. 23, no. 18, 2021.

[7] M. S. Jalali and J. P. Kaiser, "Cybersecurity in Hospitals: A Systematic, Organizational Perspective," *J Med Internet Res*, vol. 20, no. 5, 2018.

[8] L. Kessem, "Threat Actors' Most Targeted Industries in 2020: Finance, Manufacturing and Energy," Security Intelligence, 31 03 2021. [Online]. Available: https://securityintelligence.com/posts/threat-actors-targeted-industries-2020-finance-manufacturing-energy/. [Accessed 23 05 2022].

[9] E. M. Raineri and T. Fudge, "Exploring the Sufficiency of Undergraduate Students' Cybersecurity Knowledge Within Top Universities' Entrepreneurship Programs," Journal of Higher Education Theory and Practice, vol. 19, no. 4, pp. 73-92, 2019.

[10] J. Deal, "Hacking OPM," National Review, vol. 13, no. 23-24, p. 67, 2015.

[11] G. Karol, "Cyber-Attacks Cost Small Businesses Nearly $9,000," Fox Company, 22 03 2016. [Online]. Available: https://www.foxbusiness.com/features/cyber-attacks-cost-small-businesses-nearly-9000. [Accessed 24 05 2022].

[12] S. M. Kennison and E. Chan-Tin, "Taking Risks With Cybersecurity: Using Knowledge and Personal Characteristics to Predict Self-Reported Cybersecurity Behaviors," *Front. Psychol.*, vol. 11, p. 546546, 2020.

[13] N. A. A. Rahman, I. H. Sairi, N. A. M. Zizi and F. Khalid, "The Importance of Cybersecurity Education in School," *International Journal of Information and Education Technology*, vol. 10, no. 5, pp. 378-382, 2020.

[14] K. Cabaj, D. Domingos, Z. Kotulski and A. Respício, "Cybersecurity education: evolution of the discipline and analysis of master programs," *Computers & Security*, vol. 75, no. 3, 2018.

[15] F. Schneider, "Cybersecurity Education in Universities," *IEEE Secur. Priv.*, vol. 11, pp. 3-4, 2013.

[16] V. Švábenský, J. Vykopal and P. Čeleda, "What Are Cybersecurity Education Papers About? A Systematic Literature Review of SIGCSE and ITiCSE Conferences," in SIGCSE, Portland, 2020.

[17] InfoSec, "Cybersecurity Conferences 2022 – 2023," InfoSec, 2022. [Online]. Available: https://infosec-conferences.com/. [Accessed 25 05 2022].

[18] K. Stouffer, T. Zimmerman, C. Tang, J. Lubell, J. Cichonski and J. McCarthy, Cybersecurity Framework Manufacturing Profile, NISTIR 8183, U.S. Department of Commerce, 2017.

[19] W. Newhouse, S. Keith, B. Scribner and G. Witte, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, NIST - U.S. Department of Commerce, 2017.

[20] G. Jin, M. Tu, T.-H. Kim, J. Heffron and J. White, "Evaluation of Game-Based Learning in Cybersecurity Education for High School Students," *Journal of Education and Learning*, vol. 12, no. 1, pp. 150-158, 2018.

[21] M. Mylrea, S. N. G. Gourisetti and A. Nicholls, "An Introduction to Buildings Cybersecurity Framework," in 2017 IEEE Symposium Series on Computational Intelligence (SSCI), 2017.

[22] M. Dawson, "Applying a holistic cybersecurity framework for global IT organizations," *Business Information Review*, 2018.
[23] A. S. Sohal, R. Sandhu, S. K. Sood and V. Chang, "A Cybersecurity Framework to Identify Malicious Edge Device in Fog Computing and Cloud-of-Things Environments," *Computers & Security*, 2017.

Sources of funding for research presented in a scientific article or scientific article itself

There have been no sources of funding for the current article

Creative Commons Attribution License 4.0 (Attribution 4.0 International , CC BY 4.0)