DOI:10.17951/h.2022.56.1.119-142

A N N A L E S
UNIVERSITATIS MARIAE CURIE-SKŁODOWSKA
LUBLIN – POLONIA

VOL. LVI, 1 SECTIO H 2022

ŁUKASZ WIECHETEK

lukasz.wiechetek@umcs.pl
Maria Curie-Skłodowska University. Faculty of Economics
5 Maria Curie-Skłodowska Sq., 20-031 Lublin, Poland
ORCID ID: https://orcid.org/0000-0001-7755-2282

MAREK MĘDREK

marek.medrek@umcs.pl
Maria Curie-Skłodowska University. Faculty of Economics
5 Maria Curie-Skłodowska Sq., 20-031 Lublin, Poland
ORCID ID: https://orcid.org/0000-0001-5752-5084

Human Factors in Security – Cybersecurity Education and Awareness of Business Students

Keywords: computer security; cybersecurity; cybersecurity awareness; security education; cybersecurity education; business students

JEL: L86; M20; D83

How to quote this paper: Wiechetek, Ł., & Mędrek, M. (2022). Human Factors in Security – Cybersecurity Education and Awareness of Business Students. *Annales Universitatis Mariae Curie-Skłodowska, sectio H – Oeconomia*, Vol. 56, No. 1.

Abstract

Theoretical background: The rapid development of Internet interactions and a growing number of information technology users caused by digital society development and accelerated by the COVID-19 pandemic yield the significant growth of cyber-attacks and cybersecurity incidents. Members of Generation Z use information technology as a main tool for broadening their knowledge and skills. For such digital natives, proficiency in ICTs appears as an indispensable element of life. This is even more apparent during the COVID-19 pandemic, when they are forced to use IT tools more often, both for the entertainment, education, and work. Such acceleration generates new possibilities, but also new threats.

Purpose of the article: The aim of the paper is to check if members of Generation Z are aware of cybersecurity issues and whether they know basic threats and methods/tools that can improve the safety. We analyse students' behaviour in the event of cyber incident and examine whether the analysed group is willing to improve cyber knowledge, skills, and attitudes.
Research methods: We explored data collected from business students ($N = 182$). The online questionnaire was prepared in LimeSurvey. Finally, data analysis and visualization were performed in Microsoft Excel and Tableau.
Main findings: The analysis indicates that business students have rather poor knowledge in cybersecurity. The results demonstrate the need for targeted educational campaigns and trainings that address the specific cyber weaknesses to build secure ecosystem, combining both technical, organizational, and behavioural aspects.

Introduction

Many critical infrastructures including, water, food, communication, healthcare, energy distribution depends on reliable data and trustworthy IT systems and may be a victim of cyberattack (Venkatachary et al., 2018; Cassotta & Sidortsov, 2019; Arcuri et al., 2020). The security of these systems depends not only on hardware and software, but also well-educated staff and managers. Nowadays, not only the big IT, financial or telecommunication companies, but also local and central administration and finally, every single IT user can be a target of cyber-attack. People can be attacked during entertainment, education, or work. To minimize the risk of the cyber incident and its negative impact, IT users should be aware of the incident, know methods and tools that can be used to protect digital assets, and finally know how to behave in case of the incident (Zwilling et al., 2020; Zhang-Kennedy & Chiasson, 2021; Tirumala et al., 2019).

Many reports indicate that due to the pandemic situation the number of cyberattacks significantly increased. More incidents are connected not only with the increasing number of remote workers, introduction of 5G communication that allow to connect IoT devices that are prone to cyberattacks, but also with the lack of appropriate competencies of information technology users. According to the Gartner report, information security market will be worth about USD 170 billion in 2022 (Gartner, 2018) and the total cost of globally committed cybercrimes will reach USD 6 trillion by 2021 (Cybint, 2020). Almost 95% of cybersecurity incidents are caused by human error and the hacker attack is conducted every 39 seconds. For example, in the United States, the COVID-19 pandemic caused 300% increase in reported cybercrime. The increase was caused mostly by moving workers (students) from office (schools) to personal homes that use vulnerable computer networks. Market reports present a huge increase in cybersecurity incidents, caused by many technical, organizational, and human-related factors, but indicate also that human intelligence and comprehension is one of the best defenses against cyber incidents (Cybint, 2020).

One of the biggest issues is also raising cybersecurity gap (Arora & Mendhekar, 2021; Crumpler & Lewis, 2019; Kreider & Almalag, 2019) which is caused mainly

by the fact that educational programs do not keep up with the rapid technological changes. Therefore, it is a great need to explore educational programmes in cybersecurity and monitor knowledge, skills, and attitudes not only among the IT specialists, but also broad group of information technology users.

In this paper, the authors examine cybersecurity awareness of Generation Z members on the example of Polish business students. Young people, members of Generation Z born after 2000, use information technology as a main tool for broadening knowledge and skills. They were born in the Internet era, know and like to use ICTs, however not all of them may have an appropriate knowledge and skills in cybersecurity, and, therefore, can be a weak point in cyber ecosystem, so there is a strong need to constantly explore, monitor and improve their digital competences.

This paper is divided into three parts. Firstly, the authors present literature research addressing the cybersecurity education. Secondly, the examples of coordinated actions in cybersecurity undertaken by the Polish government and universities are given. Finally, cybersecurity knowledge, skills and attitude of Polish business students, members of Generation Z are analyzed. The main part of the paper presents the methodology, research sample, collected data and research outcomes in cyber education. At the end, the conclusions and recommendations, both for the university authorities, academics and business representatives, are presented.

Cybersecurity education

The Internet is a worldwide computer network which brings many IT security threats and challenges. There are numerous publications about cybersecurity, however, not many addressing security awareness and the individual indifferences in cybersecurity behavior (Whitty et al., 2015). To find out how the extent of the issues of cybersecurity education is reflected in the scientific literature, the authors analyzed titles of 642 full text scientific articles indexed in EBSCO (https://www.ebsco.com). The analyzed titles contained 1,325 unique, interpretable words with more than three characters. The most frequent words used to entitle cybersecurity-related articles were shown in Figure 1.

The word cloud presents only words that were used more than five times. As we can see, the cybersecurity articles were devoted mainly to information security, the Internet and data. Many articles also addressed the risks related to cybersecurity, possible threats like privacy violation, impacts on industry and organizations. Other important issues were security analysis, developing strategies, building systems for better protection against attacks. Although the search phrase "cybersecurity" or "cyber security" used in Business Searching Interface returned 642 full text articles, among them only few were related to cybersecurity education and awareness.

Figure 1. The most frequent terms used in titles of cybersecurity-related scientific papers

Source: Authors' own study.

The analysis shows that there is great need for teaching students not only technical side of IT security, but also its organizational and behavioral aspects, related to the safe use of the computer technology. The security issues should be incorporated not only into IT courses (for programmers, system administrators, network specialists, security specialists), but also for managers to stress organizational and behavioral aspects of cybersecurity (Affisco, 2017). Organizational, behavior theories and concepts are necessary for understanding the attitudes towards IT security, however, most of the technology users, including business students, do not know how important cybersecurity is nowadays (Affisco, 2017). The interdisciplinary nature of cybersecurity education is also presented in the National Initiative for Cybersecurity Education (NICE), that can act as a reference source for organizations that want to develop cybersecurity workforce (Newhouse et al., 2017).

Many researchers have performed studies to explore connections between education and cybersecurity awareness of pupils, professionals, and senior citizens (Tirumala et al., 2019; Pendley, 2018; Blackwood-Brown et al., 2021; Pencheva et al., 2020) and study programs and cybersecurity topics they covered (Cabaj et al., 2018). Imgraben et al. examined 250 smart mobile device owners and found that participants did not notice the risks and not perceived cybercrime as a real threat. They recommend organizing training programmes concerning basic online security and awareness programmes to promote security culture (2014). Security threats have negative impact not only on assets of an organization but also on its reputation. Dahbur et al. examined private and public organizations in Amman and showed that security awareness level is similar for all positions and for all lengths of employment. Therefore, it is necessary to raise cybersecurity issues during the study programmes to provide on the market well-trained employees with a high awareness of IT security. The authors recommend development and promotion security trainings tailored to

concerns of given organization. Organizations should also prepare information as far as possible in many forms like mail reminders, LMS systems, newsletters but also conduct security awareness workshops (Dahbur et al., 2017).

In the field of cybersecurity, human behavior seems to be the weakest link (Alqahtani & Kavakli-Thorne, 2020). Both awareness and education have a big impact on cybersecurity level. McCrohan et al. (2010) examined users' passwords and ways of securing computers pre and post cybersecurity training. They stated that education of the threats related to e-commerce and showing proper security practices changes the behavior of online customers, improves their own cybersecurity and security of their employers.

For obtaining better results, the course content should be prepared according to the student's profile. However, the next important thing is also the delivering method. Abawajy (2014) explored user preference of cybersecurity awareness delivery methods. The researcher shows a wide range of delivery methods: online trainings, contextual training and embedded training, and concludes that combined delivery methods (text-, game-, and video-based) are better than individual delivery methods. The effective way of learning can be gamification (Demmese et al., 2020; Ros et al., 2020). The raising interest in game-based cybersecurity learning was reported in Jin et al. (2018), Gonzalez et al. (2017), Jorgensen et al. (2017) and Alqahtani et al. (2020). Also, Pawlowski and Jung (2015) examined students' concern about cybersecurity threats and identified 23 concepts forming understanding of cybersecurity. They advise that cybersecurity courses should be problem-centered, utilizing case studies, and tailored to students' level of awareness.

Also, Son et al. (2015) confirmed that cybersecurity teaching can be organized in different ways. They described the process of integrating security labs into curriculum in three forms: a pure virtual lab, the traditional physical lab, and a hybrid approach. They conclude that security labs should be essential part of the curriculum, however, the deployment model should be based on individual institutional requirements. The curriculum should be practical to motivate students, increase the retention and enrolment. Cybersecurity threats are still changing, so course programmes should be flexible and include emerging cybersecurity topics and possible to teach at different levels of education. That kind of strategy was proposed by Harris (2015). The researchers developed cybersecurity taxonomy that allows to move security issues from higher level courses to lower and intermediate courses. Their IT security taxonomy was based on Bloom's and Webb's taxonomy.

Cybersecurity education is required in today's virtual, digital and network connected world. Cybersecurity is not a state but a continuous process. As literature shows, courses should be prepared not only for IT specialists but also managers, office workers or just casual users of information technology of different age. Course attendants should be both young children, teenagers, employers but also older people because the cyber-attacks should be the concern to all members of the information society. Trainings must be interesting, i.e. prepared in different forms, and use var-

ious delivery methods like gamification. The main aim of the program should be to increase the awareness of cybersecurity threats.

Cybersecurity education in Poland

To undertake long-term and coordinated actions in the field of cybersecurity, the Polish Ministry of Digital Affairs developed "The Strategy of Cybersecurity of the Republic of Poland for the Years 2017–2022". The main aim of this document is to ensure a high level of security for the public sector, private sector and citizens who use digital services (Ministry of Digital Affairs, 2017). The document presents the actions that should be taken in order to:

– achieve capacity for nationally coordinated actions to prevent, detect, combat, and minimize the impact of incidents that compromise the security of ICT systems,

– enhance the ability to fight cyber threats (including cyber espionage and cyber terrorism) by building better analysis methods, secure communication system and improvement of security audits and tests,

– enhance national capacity and cybersecurity competencies by developing infrastructure, increase cooperation between public and private sector, stimulating R&D actions in the area of cybersecurity,

– build strong international position in the field of cybersecurity by active international strategic cooperation but also operational and technical partnership.

One of the possible ways of this strategy implementation and improving cybersecurity awareness is incorporating IT security into Polish educational system. Primary and secondary schools take action to increase awareness in cybersecurity. Due to the increase in the cyber threats, the Polish Ministry of National Education (2017) advices to organize special meetings and trainings for parents and children on the safe use of the Internet. According to the Polish law regulation, schools that offer Internet access are obliged to protect pupils against accessing to inappropriate content, also must install and update security software. Educational system must promote cyber safety awareness and to develop appropriate attitudes towards threats related to the use of information and communication technologies. It is also planned to develop Nationwide Education Network – virtual public telecommunication network that will help to protect users from network threats in a manner and scale unattainable by telecommunications operators.

Polish universities and business schools continue to increase cybersecurity awareness. They offer cybersecurity study programmes. Table 1 contains the description of sample cybersecurity courses offered by Polish universities and high schools.

Table 1. Sample cybersecurity courses offered by Polish universities

Course title	Duration	Course description
"Cybersecurity"	2 terms, 200 hours, postgraduate	University curriculum prepared with cooperation with cybersecurity experts, and companies. It offers knowledge and practical skills in: – legal aspects – auditing IT systems – hazard identification – preventive actions – prevention of attacks – creating procedures and supervising processes – investigative analysis and data recovery – techniques and tools related to cybercrime
"Cybersecurity and Protection of Information Resources"	5 modules, 180 hours, postgraduate	The aim of the study is to provide knowledge and good practices in cybersecurity, as well as the legal, organizational, and technical security methods. The study includes: – public information resources and their computerization – cyberspace protection – personal data protection – protection of classified information – criminal responsibility
"Cryptology and Cybersecurity"	7 terms, Engineering studies	Curriculum covering software engineering, programming languages and techniques, classical cryptanalysis, accreditation and certification of devices and cryptographic systems, wireless security, HTML and web applications, cryptography applications on the Internet. Students learn how to design and operate various types of security systems, work in interdisciplinary teams and identify hazards. Student can choose one of three specialties: – cyber defense – information security – cryptographic systems
"Cybersecurity – Standards and Good Practices"	Bachelor programme	The aim of the study is to achieve comprehensive knowledge of principles, standards, and good practice in maintaining organization safety. The study program is based on accredited professional frameworks and prepares for international certification. The course includes: – international security standards – recognition and protection against social attacks – good practices in IT audit governance – information security – advanced aspects of building security in organizations – IT risk – IT teamwork
"Cybersecurity Management"	2 terms, postgraduate	Studies covering a broad spectrum of cybersecurity issues for beginners or intermediate attendants. Students do not need to know technical issues related to the security of information systems. Classes are conducted with cooperation with practitioners from IT security companies. The course includes: – introduction to cybersecurity – cybersecurity risk management – data and information security management – technological aspects of cybersecurity – future of cybersecurity
"IT Cyber Security"	Master programme, 2 years	Program combining knowledge of computer science with knowledge of political science and administration. The course includes: – the place of cybersecurity and security issues – political, legal, economic, and sociological aspects of security – principles of operating systems and computer networks – secure web application programming – cryptographic methods and modules – security tests and audits – standards for information security management

Source: Authors' own study.

Most of the courses offered are postgraduate studies. They mostly address technical aspects of cybersecurity, but also international standards, law regulations and security tests and management. Many courses were prepared with the cooperation with the security companies and organizations operating on Polish IT market. The university staff members are frequently assisted by practitioners, experts in the cybersecurity domain.

However, many schools and universities do not have the typical cybersecurity courses addressing organizational, procedural, and behavioral cybersecurity issues. They supplement their courses in the area of IT (e.g. management information systems, business informatics, information management) with topics related to information security. Cybersecurity courses are provided mostly for IT students and IT specialists (postgraduate studies). However, we can observe lack of courses addressing knowledge and "soft" skills prepared for business students that in the future will become managers, owners of companies and organization who will have to deal with many cybersecurity threats.

We can state that cybersecurity issues are very important for Polish authorities. The actions to improve the cybersecurity level are taken both at the strategic, tactical, and operational level. An important element of implementation of the cybersecurity strategy is the incorporation of numerous security issues into educational programs at all stages. All of the above efforts are made to increase cybersecurity awareness and build strong, resistant cyber ecosystem. However, the above-mentioned incentives and actions are quite new, and we need time to see the results. Information technology is developing rapidly. New technologies are used to implement IT systems and application, also the number of ICT users increases very fast, and, therefore, to identify and minimize the cyber gap, more and more research in cybersecurity, addressing not only technical issues, but also an organizational and procedural aspect of cybersecurity is still needed. To build wide knowledge, strong skills, and appropriate behavior, the first cyber trainings should be introduced quite early before the high school stage, preferably primary and secondary schools, or maybe even in kindergarten (Rahman et al., 2020; Corradini & Nardelli, 2020; Siddiqui & Zeeshan, 2020), and then constantly enhanced during the next stages of education and professional development.

In the next parts of the article, the authors analyze data collected from Polish business students to know their previous, current, and future cybersecurity educational achievements. The aim of our research is to check the level of their cybersecurity awareness and the preferred ways of improving the cyber knowledge, skills, and attitudes, and, finally, know their willingness to improve the cyber skills.

Methodology and research

The research procedure and questions

The research framework has been divided into the following stages: literature analysis, research questions, survey preparation, data gathering, statistical analysis, final conclusions, and future work. The scheme of the procedure is presented in Figure 2.

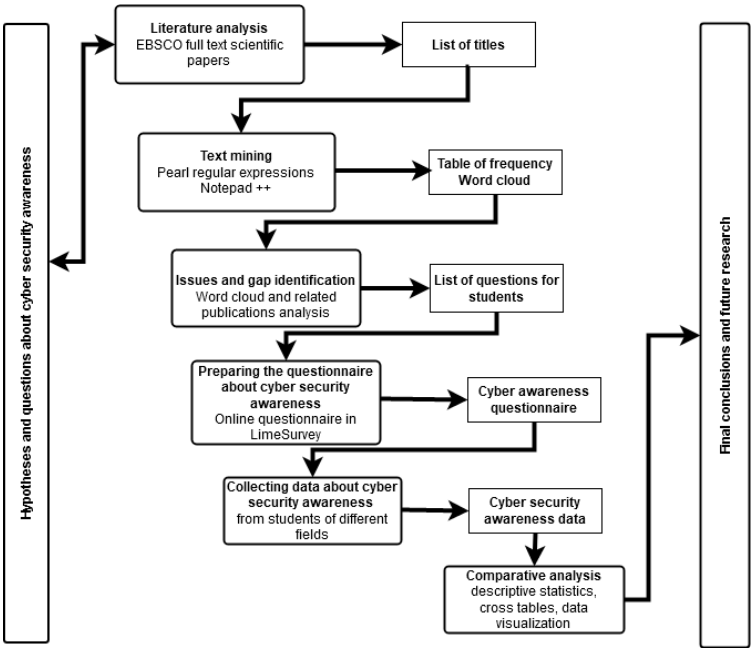

Figure 2. The research on cybersecurity

Source: Authors' own study.

Information collected at the literature analysis stage (described in Section 1 and Figure 1) was used for preparing the survey for Generation Z students from Poland. The questionnaire was prepared in LimeSurvey, an open-source web application for developing online surveys and the hyperlink to the questionnaire was sent to students from the Faculty of Economics, MCSU (Poland). Finally, data analysis and visualization were performed in Microsoft Excel and Tableau.

The literature research and the analysis of high school curriculums allowed to develop the following research questions:

– Are business students aware of security issues?
– What are the main sources of knowledge about cybersecurity?
– Do young people know basic IT security threats?
– Do students know basic methods and tools for improving IT security?

– What are the differences in cybersecurity between the groups of Polish students?
– Do young people want to improve their knowledge and skills in cybersecurity?

To answer the research questions, the online questionnaire was prepared. The questionnaire consisted of 33 questions regarding:

– understanding the "cybersecurity" term,
– willingness to use IT technologies,
– means and tools used to avoid cyberattacks,
– knowledge and skills that positively affect the level of cybersecurity,
– behavior in case of the cyberattack,
– past, current and future cybersecurity education,
– respondent characteristic.

The analysis of the responses collected from business students was described in the "Data analysis and the results" section.

The characteristics of the respondents

To get the answers to the research questions, the authors collected data from young people, members of Generation Z – business students. The online survey was completed by 182 students. The characteristics of the respondents was shown in Table 2.

Table 2. The characteristics of the respondents

Characteristics (N = 182)		N	%
Gender	Female	97	53.30
	Male	85	46.70
Type of study	Full-time study	174	95.60
	Part-time study	8	4.40
Year of study	First-year Bachelor	117	64.29
	Second-year Bachelor	13	7.14
	Third-year Bachelor	6	3.30
	First-year Master	33	18.13
	Second-year Master	10	5.49
	PhD student	3	1.65
Field of study	Business analytics	26	14.29
	Economics	34	18.68
	Information technology	3	1.65
	Logistics	105	57.69
	Management	14	7.69

Source: Authors' own study.

Among 182 students slightly over 53% of them were male students, most of them (95%) were full-time students. Most of the respondents were first-year Bachelor. They were mostly students of Logistics (58%), Economics (19%) and Business analytics (14%).

Data analysis and the results

Cybersecurity understanding and familiarity

At the beginning of the questionnaire, the respondents were asked to perform a cybersecurity self-assessment. On the scale from 1 – *no knowledge* to 5 – *very good knowledge*, they characterized the level of their familiarity with the "cybersecurity" term (Figure 3).

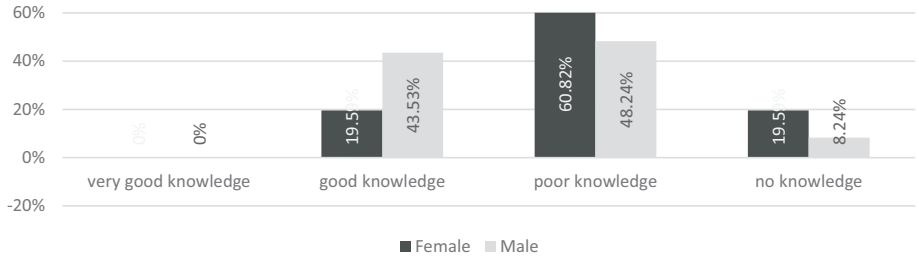

Figure 3. Level of cybersecurity knowledge by gender (self-esteem)

Source: Authors' own study.

None of the students reported very good knowledge in the field of cybersecurity. Most of the respondents indicated poor knowledge or no knowledge in this area (respectively 55% and 14%), only 31% reported good knowledge. Analyzing the gender, more familiar with cybersecurity issues were male respondents – about 44% with good knowledge while only 20% of female students indicated good knowledge in this area. This shows that cyber skills of business students must be supplemented and improved. Not only because of fast development of IT solutions, but also because of shortcomings in the basics of cybersecurity in a group of business students. The students' cybersecurity self-esteem was presented in Figure 4.

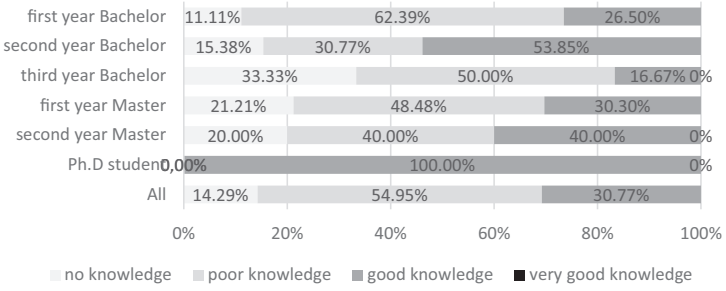

Figure 4. Level of cybersecurity knowledge by the year of study (self-esteem)

Source: Authors' own study.

We are unable to show a simple relation between a year of study and increasing knowledge in the field of cybersecurity. The higher level of cybersecurity knowledge was declared by second-year Bachelor and second-year Master students. However, third-year Bachelor students reported mostly poor and no knowledge in this area. All the PhD students also reported good knowledge of cybersecurity. Analyzing the above results, we can assume that lack of progress in this area may be caused by lack or not enough emphasis on the cybersecurity issue in the courses enclosed in the study programme or poor quality of education in this area. However, to confirm this assumption, more research exploring IT-related study programmes that provide cybersecurity trainings like computer network administration, application development or database design, is needed.

The respondents were asked to indicate three terms that they associate with cybersecurity. The results are shown in Figure 5.

Figure 5. Terms associated with cybersecurity

Source: Authors' own study.

Among 516 terms indicated by the respondents the top five were "password" (8.9%), "antivirus" (8.3%), "security" (5.4%), "safety" (2.7%) and "firewall" (2.3%). We conclude that the students are aware of basic mechanisms like strong passwords or dedicated software that can increase the security level. The terms that appeared less frequently in surveys (less than 1%) were: "industrial safety", "ad blocker", "social media", and "account". It may indicate that young business students notice both the problems of single Internet users like identity theft, but also indicate the threats for business, industry, and intelligent networks.

The respondents also indicated three devices that are prone to cyberattacks. The most common devices that in respondents' opinion are prone to cyberattacks are computers, smartphones, tablets, and laptops. However, some respondents also indicated wearables, TV, ATMs, and routers. That type of hardware was reported quite rarely, less than 0.5%. The results show that members of Generation Z clearly notice the need of securing personal devices computers, smartphones, and tablets, however, more education is needed to transform awareness into action and deliver broad knowledge and skills on how to build secure ecosystem consisted of many common devices, computers, smartphones but also other devices that are frequently used and can be hacked too (wearables, TVs, Bluetooth hardware and network hardware).

The main sources of knowledge about cybersecurity

To show preferred sources of cybersecurity knowledge, the respondents could choose more than one option from the following list: websites, social media, talking with friends, university classes, radio, television (traditional media), IT journals, industry reports, scientific journals and being a victim of cyberattack. The most indicated sources were web pages (80%), social media (65%), talking with friends (45%) and university classes (41%). The less popular sources, chosen by less than 10% of the respondents were: scientific journals, industry/business reports, and being a victim of cyberattack (Figure 6c).

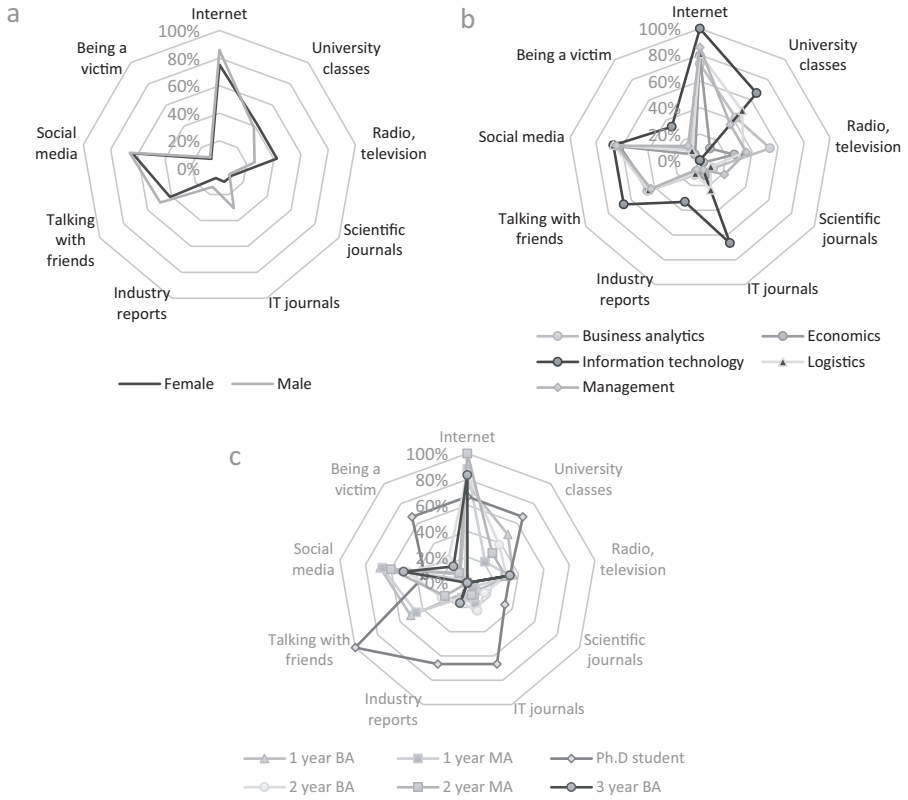

Figure 6. The main sources of knowledge about cybersecurity for different: genders (a), fields of study (b) and years of study (c)

Source: Authors' own study.

The male respondents often emphasized web portals and IT journals (86% and 31%) as the main cybersecurity sources, while only 75% and 10% of female respondents used these sources (Figure 6a). There were no significant differences between students of different years of studies, except that MA/MSc students more frequently

(90%) indicated web portals as the main source of knowledge, while only 76% of young first-year Bachelor students indicated this source. Talking with friends was the most popular source of information among PhD students (Figure 6c). The results show that the university cannot be recognized as the main source of information about cybersecurity.

Known threats and tools for improving IT security

On a scale from 1 (*strongly disagree*) to 5 (*strongly agree*), the respondents could assess the main cybersecurity threats. The list of possible threats included: blocking access to information, violation of privacy, loss of data, loss of money, device damage, spying people, spying organizations, influencing the social choices, unauthorized takeover of devices, blocking business processes, attacks on IT infrastructures (power grids, railways), using IT infrastructure for terrorist attacks, knowing personal details, and knowing consumer behavior preferences. Table 3 presents the results of the survey grouped by gender, study level and fields of study of the respondents.

Table 3. The main cybersecurity threats – survey results by gender, study level and fields of study of the respondents

	Gender		Study level						Fields of study					
Threats	Female	Male	1 year BBA	2 year BBA	3 year BBA	1 year MA	2 year MA	Ph.D student	Business analytics	Economics	Information technology	Logistics	Management	***Average for threats***
Influencing the social choices (elections)	3,4	3,5	3,4	3,2	3,8	3,7	3,7	3,3	3,5	3,4	4,3	3,4	3,6	***3,4***
Blocking business processes	3,4	3,6	3,5	3,1	2,8	3,6	3,8	3,7	3,5	3,6	3,0	3,5	3,7	***3,5***
Unauthorized takeover of devices	3,4	3,7	3,4	3,6	3,8	3,8	3,8	3,3	3,5	3,6	3,7	3,5	3,8	***3,5***
Blocking access to information	3,4	3,7	3,5	3,3	3,2	3,6	3,7	3,7	3,3	3,8	2,7	3,5	3,6	***3,5***
Knowing my consumer behavior preferences	3,5	3,7	3,5	2,7	4,0	3,8	3,7	3,7	3,3	3,6	4,0	3,6	3,4	***3,6***
Attacks on IT infrastructures (pow er grids, railw a	3,6	3,6	3,6	3,4	3,5	3,7	3,8	4,0	3,4	3,5	3,3	3,7	4,0	***3,6***
Device damage	3,7	3,7	3,6	3,5	4,0	3,8	3,9	3,0	3,5	3,7	3,3	3,7	3,9	***3,7***
Spying people	3,6	4,0	3,8	3,6	4,2	3,8	3,8	3,7	3,7	3,6	3,3	3,9	3,5	***3,8***
Spying organizations	3,6	3,9	3,7	3,8	3,8	3,9	3,9	4,0	3,5	3,6	3,7	3,9	4,0	***3,8***
Knowing my personality details	3,6	3,9	3,8	3,0	4,0	4,1	3,8	3,7	3,4	3,9	4,0	3,9	3,7	***3,8***
Use IT infrastructure for terrorist attacks	3,8	4,0	3,9	3,3	3,2	3,8	4,3	4,0	3,6	3,6	3,7	3,9	4,1	***3,9***
Loss of data	3,7	4,1	3,9	3,5	3,3	4,2	4,0	4,3	3,7	4,0	3,0	3,9	4,1	***3,9***
Violation of privacy	3,8	4,0	3,8	3,8	3,5	4,3	4,0	4,3	3,5	4,1	4,0	3,9	4,0	***3,9***
Loss of money	3,8	4,1	3,9	4,1	3,5	4,2	4,1	4,0	3,5	4,1	3,3	4,0	4,0	***3,9***
Average for the group of respondents	***3,6***	***3,8***	***3,7***	***3,4***	***3,6***	***3,9***	***3,9***	***3,8***	***3,5***	***3,7***	***3,5***	***3,7***	***3,8***	

Source: Authors' own study.

The main threats indicated by the respondents were loss of money, violation of privacy, loss of data and the possibility to use IT for terrorist attack (the last column of Table 3, average >3.8). The less important were influencing social choices, blocking access to information and business processes, and, finally, unauthorized takeover of

devices. The average score for these items was less than or equal 3.5. We can observe also higher importance of all the threats (except for attacks on IT infrastructure) by male students. The biggest differences were observed in spying people and organizations, losing money and data (more than 7%).

Analyzing the year of the study, we can notice the stronger impact of cyber threats reported by Master programme students (average for the group of respondents equals 3.9). For Bachelor students, the average was between 3.4 and 3.7. We cannot observe the influence of the year of study and the perception of the main cyber threats. Such weak relation can be explained by the lack of expected cybersecurity classes in the study programmes. If the student got appropriate knowledge and skills during the classes the correlation between the perception of main cyber threats and the study year could be positive or negative, but clear. If the students had more knowledge of cybersecurity threats, and the prevention of how to avoid them was weak, the respondents would rather indicate their greater impact. On the other hand, when the students were provided with necessary knowledge, but also skills and attitudes that will allow them to secure the cyber activities, they would probably report lower impact of cybersecurity threats.

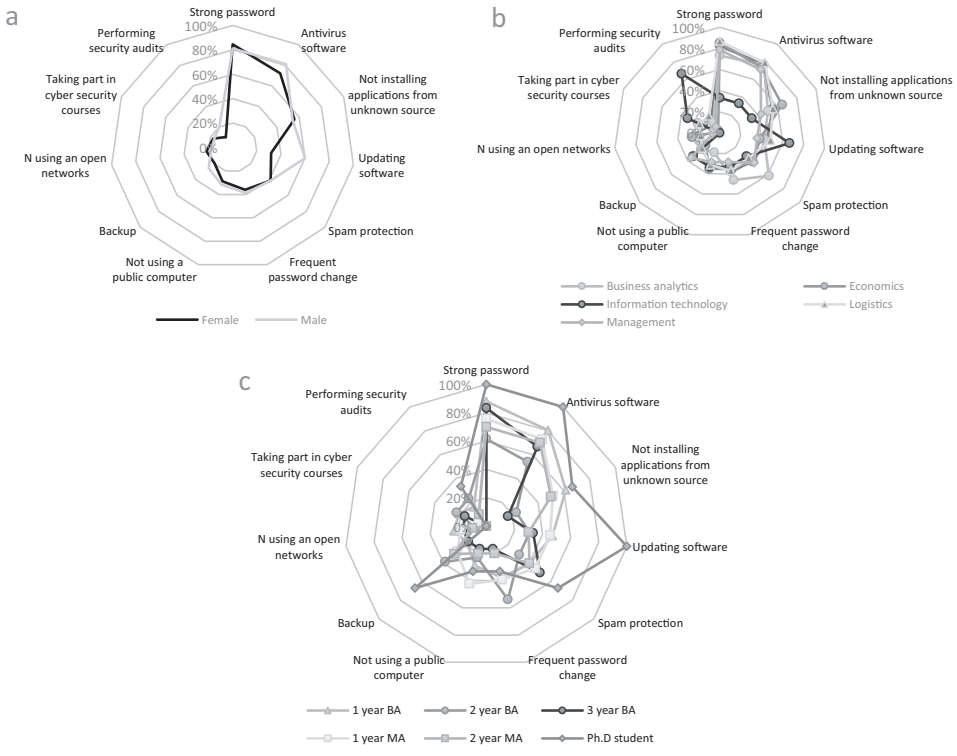

Figure 7. Means used to avoid cyberattacks for different: genders (a), fields of study (b) and years of study (c)

Source: Authors' own study.

In addition, the respondents indicated means that they used to avoid cyberattacks (Figure 7). They could choose more than one item from the following list: strong password, frequent password change, updating software, making backups, antivirus software, spam protection, not using a public computer, not using an open network, attending cybersecurity courses, performing computer security audits, and not installing applications from unknown sources.

Among the most frequently used methods and tools for improving the cybersecurity, the following were recognized: strong password (83%), using antivirus software (76%), and not installing the applications from the unknown source (55%). The mechanisms used by female and male students and the frequency of its usage was quite similar except for software updating – only 32% of female respondents used this method, while 60% of male students performed software updates. Analyzing the types of studies, we notice that IT students more often performed security audits, took part in security courses, and used software update. Business analytics students more frequently changed their passwords and used anti-spam software. According to the year of study, PhD students used the most security tools, while the third-year bachelor students reported that they used security mechanisms less frequently. Since the analysis indicated that the most popular are simple methods, based on password and antivirus software, the cybersecurity courses should widen the catalog of security mechanisms, e.g. using passwords managers, avoiding public networks and computers, regular backup and performing the security audits. As technology development is accompanied by little commitment to cybersecurity courses, the study programmes should enable and encourage students to continuous improvement of cyber competences.

Finally, the respondents were asked about their behavior in case of cyberattack and what people or organizations would they inform in that case. They could choose on out of five options: *yes sure – definitely*, *rather yes*, *I have no opinion (indifferent)*, *rather no*, *definitely no* (Figure 8).

We can observe that the respondents were polarized. 42% reported that they rather know how to behave and 29% stated that they probably would not know what to do in case of the attack. There were not big differences in terms of the gender, but female respondents were more determined (only 13% no opinion answers), however, they more frequently reported lack of knowledge about how to behave. Also, Information technology students were more sure how to behave (67%), while the majority of Management students did not know how to act in case of a cyberattack (57% of students answered *rather no* and *definitely no*). Analysis of study year also did not indicate a clear relation between knowledge and the study year and level. There can be stated that also in this case we can observe the deficiencies in the curricula. In study programmes addressing IT security issues we should have more students who know how to behave in the later years of study, especially Master and PhD students should know exactly know how to behave. Once again, we could notice the gap in study programmes for business students. To fill in this gap, the syllabuses should be supplemented with the methods and tools increasing the cyber security level, but also procedures and recommendations how to act or communicate in case of a cyberattack.

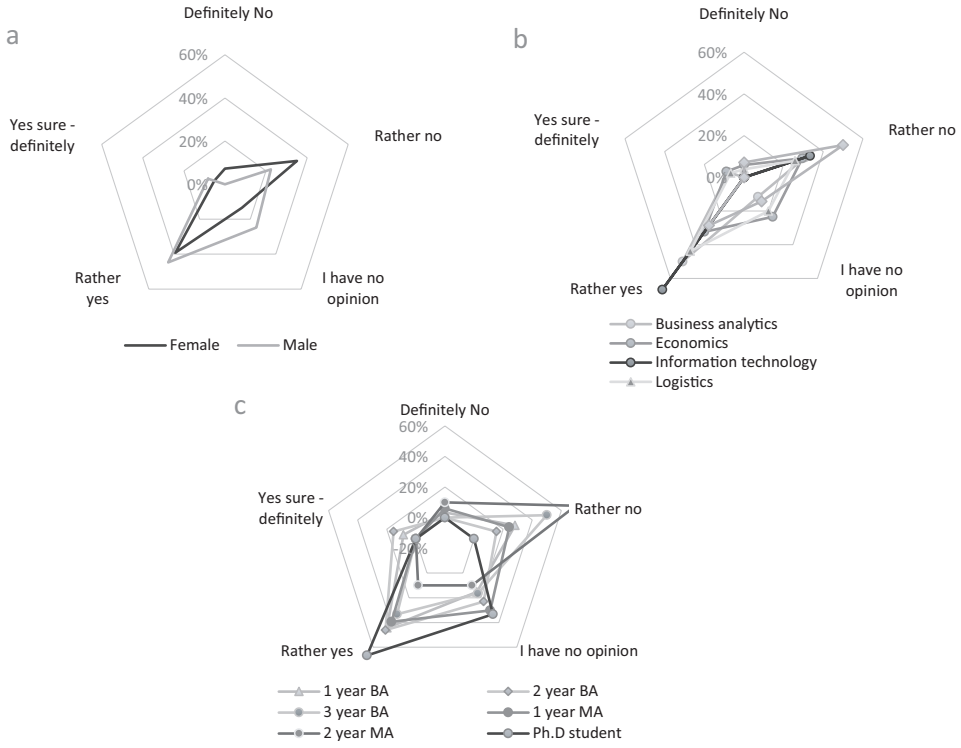

Figure 8. Knowledge of how to behave in the case of a cyberattack

Source: Authors' own study.

It is also important for users to know who to inform in case of such an incident (Figure 9). The students could indicate one or more answer from the list: best friend, parents, police, bank, boss, university teacher, friends on social network, nobody.

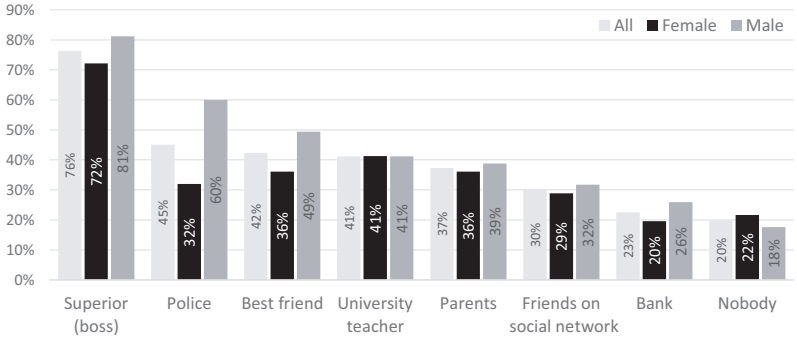

Figure 9. Organization/people to inform in the case of a cyberattack

Source: Authors' own study.

Most of the respondents (76%) would inform their boss. Second, the most popular choice was the police (45%) and best friend (42%). However, still about 20% of students declared that they will not inform anybody. The male respondents were more willing to inform other people or organizations about being a victim of a cyberattack. Especially big differences were observed in case of informing the police (male 60%, female 32%) and friends (male 49%, female 36%). This issue should be also addressed by cybersecurity courses. Not everyone will be the cyber specialist and will be able to use specialized security tools, however, in case of attack, he/she should know who should be informed to minimize the risk of the threat spreading and to have a chance for an effective defense. Building the openness and right communication in case of cyber incidents should be therefore also an important part of cyber training for business students.

Improvement of the knowledge and skills in cybersecurity

In the survey, the respondents were asked about their knowledge, skills, and behavior in cybersecurity, but also about their past, present, and future education (Figure 10, Table 4).

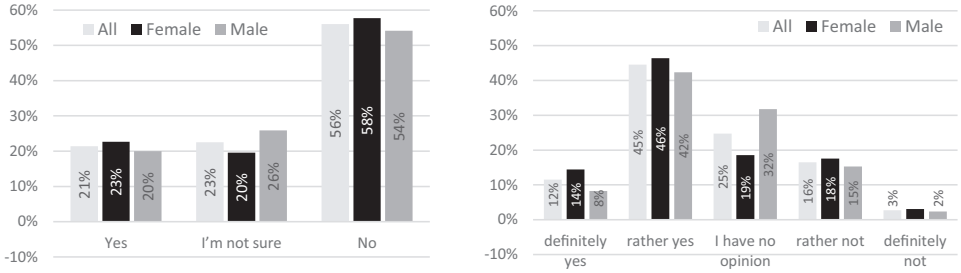

Figure 10. Previous attendance (left) and willingness to attend (right) cybersecurity trainings

Source: Authors' own study.

Most students (56%) indicated that they have not attended cyber security classes or trainings. Only slightly over 20% have taken part in those trainings. The students are also willing to attend cybersecurity classes – almost 50% would rather or attend such trainings. Only 19% were rather not interested in taking part in such trainings. As we can see, most of business students have no educational experiences in cybersecurity, also they are willing to take part in the courses. In addition, the students stated that their current education has only slightly affected their cyber security awareness (Table 4).

Table 4. Current education influence on cyber-security awareness – survey results by gender, study level and fields of study of the respondents

	Gender		Study level						Fields of study					
To what extent has your current education influenced cyber-security awareness?	Female	Male	1 year BA	2 year BA	3 year BA	1 year MA	2 year MA	Ph.D student	Business analytics	Economics	Information technology	Logistics	Management	*Average*
strongly affected	2%	0%	1%	0%	0%	3%	0%	0%	0%	3%	0%	1%	0%	***1%***
affected	20%	25%	25%	23%	17%	18%	0%	33%	19%	15%	33%	27%	7%	***22%***
hard to say	65%	53%	59%	62%	33%	58%	80%	67%	58%	65%	33%	57%	71%	***59%***
not affected	11%	16%	12%	15%	33%	18%	10%	0%	15%	18%	33%	11%	14%	***14%***
definitely not affected	2%	6%	3%	0%	17%	3%	10%	0%	8%	0%	0%	4%	7%	***4%***

Source: Authors' own study.

The results of the survey should be considered by business faculty authorities when developing or modifying study programs. Interesting is also a group of undecided respondents – 23% do not know if they attended cybersecurity trainings and 16% did not specify their future choices. That group probably consists of students that have marginal or no knowledge of cybersecurity, and, therefore, need a special attention.

Conclusions

Cybersecurity issue becomes a very important not only because of the increasing number of Internet interactions, developing new technologies that generate new possibilities and threats, but also because of the COVID-19 pandemic situation that forced people to move their entertainment, educational and professional activities online, and made the future more digital/virtual than ever.

The stereotype is that Generation Z are IT technology natives. Therefore, in this paper the authors examined the research papers addressing cybersecurity education, analyzed cybersecurity courses offered by Polish universities, and, finally, asked business students, members of Generation Z ($N = 182$) about their knowledge, skills, and behavior related to cybersecurity. Our results show that many of them may not have sufficient knowledge and skills to prevent cyberattacks and minimize their negative effects.

The performed exploratory study showed that the level of cybersecurity knowledge is rather poor. None of the respondents indicated very good knowledge and only 31% reported good knowledge. That allows for the conclusions that cybersecurity courses should be offered not only for IT students but should have broad

audience of different age. The main associations with cybersecurity are "password", "antivirus", and "safety". The respondents may know the basic methods and tools. However, they need to be educated and reminded how to effectively use it, in order to transform awareness into action. There is also a great need to stress not only the technical aspects of cyber world, but also provide procedural and organizational methods to prevent the negative aspects of cyber incidents. Students must know that cybersecurity ecosystem is very wide and includes many components like hardware, applications, usage, law, communication, education, cooperation, and, finally, that the human is one of the weakest elements in this system.

The results show that the main sources of knowledge about cybersecurity, indicated by the respondents were web pages, social media and exchanging information with friends. Therefore, cyber education should use this media and communication channels to build strong and safe cyber ecosystem based on reliable and up-to-date information. Users should know what Internet sources are safe, how to look for validated information, and who could they ask for help or just who should be informed in case of security incident. Educational process should develop a habit of fast and proper reacting to cyber threats. The main threats identified by students concerned individual users, however, the digital world is a set of strongly connected objects: users, processes, organizations, companies, sensors, each of which has a significant impact on final security. Therefore, the trainings should stress not only the threats, methods, tools that can be useful for the individuals, but give a holistic view, teach how to broadly analyze cybersecurity risk and issues related to organizations and societies.

Older students did not report more advanced knowledge and skills in cybersecurity. That may be due to lack of appropriate courses in study programmes. Therefore, if we want to better prepare business students for functioning in the digital world that seems inevitable, the study programmes should be supplemented with up-to-date, coherent trainings, with increasing difficulty level, and use gamification methods. IT users should know not only the threats and tools increasing the cybersecurity to minimize the risk, but also should know how to behave in case of the incident. To stimulate this attitude, the trainings should clearly indicate what people or organizations should be informed in case of cyberattacks, provide the right emergency procedures, but the most important seems to be creating an attitude of openness and willingness to inform specialists in the event of such an incident.

Finally, the respondents reported that they did not attend many cyber trainings in the past and are willing to take part in such courses in the future. They stress that current education do not have big influence on their cyber-security awareness. The study programmes should meet their needs and, thus, attract new students, but also educate graduates better adapted to the digital society. We must remember that cybersecurity is not a state but a continuous process. Literature shows that cybersecurity courses should be prepared not only for IT specialists, but also managers, office workers or just casual users of information systems. Course attendants should be both young children, teenagers, students, employers, but also older people because cyberattacks

should be the concern to all members of the society. Trainings should be interesting, i.e. prepared in different forms, with various delivery methods.

To improve the actual situation of cybersecurity awareness in student community, an access to open sources of knowledge should be increased by, e.g. preparing massive open internet courses (MOOCS) that will constantly provide proven and useful information regarding cybersecurity. Such widely available courses, confirmed by university prestige, could create safe places and platforms that would offer reliable and comprehensive information, understandable not only for advanced IT users. At the same time, due to the increasing use of IT technology specialized cybersecurity-related courses should appear in major university curricula – such courses could provide selected information on cybersecurity, which are especially important from the point of view of a given field of study.

Our results could be useful not only for the university authorities that are looking for the new ways and areas for improvement of the study programmes, but also academics that should know well the needs of the students and the market to prepare better course materials and offer them in the most appropriate way. Finally, the paper could be useful for company managers that have to manage the cybersecurity risk, which involves not only the use of appropriate hardware and software, but also proper development of employees' knowledge, skills, and attitudes.

Limitations

The analysis was based on the sample of business students at Maria Curie-Skłodowska University in Lublin that may limit the generalization of the results. The results cannot be directly applicable for information technology users of different age and field of studies but may supplement another research. The analysis and the recommendations were based on curricula for Polish business students. The solutions used in different countries may be based on other assumptions. Therefore, to prepare more universal recommendations in cybersecurity knowledge skills and attitudes among business students, more international, comparative analysis is needed.

Further research

The revised literature and business reports suggest that cybersecurity is nowadays a very important issue and, in the future, it will be even more significant. Cyberattacks can cause a lot of damages, have influence not only on single Internet users or companies, but also on whole economies or societies. The presented research was limited only to students' opinions, therefore, the future research is needed to get more detailed information about the cybersecurity competences of different groups of IT users (different age, various competences). Interesting case is also the impact of the COVID-19

pandemic on the cybersecurity ecosystem. During the future research, the authors would also like to explore cybersecurity education costs or willingness to pay for an extra security training. The interesting area for exploration is also new cybersecurity concerns related to the use of smartphones and the Internet by very young people.

References

Abawajy, J. (2012). User preference of cyber security awareness delivery methods. *Behaviour & Information Technology*, *33*(3), 237–248. **doi:10.1080/0144929X.2012.708787**

Affisco, J.F. (2017). Expanding cyber security learning in the business curriculum. *Proceedings for the Northeast Region Decision Sciences Institute (NEDSI)*, 420–435.

Alqahtani, H., & Kavakli-Thorne, M. (2020). Does decision-making style predict individuals' cybersecurity avoidance behaviour? In *International Conference on Human-Computer Interaction* (pp. 32–50). Cham: Springer. **doi:10.1007/978-3-030-50309-3_3**

Alqahtani, H., Kavakli-Thorne, M., & Alrowaily, M. (2020). The impact of gamification factor in the acceptance of cybersecurity awareness augmented reality game (CybAR). In *International Conference on Human-Computer Interaction* (pp. 16–31). Cham: Springer. **doi:10.1007/978-3-030-50309-3_2**

Arcuri, M.C., Gai, L., Ielasi, F., & Ventisette, E. (2020). Cyber attacks on hospitality sector: Stock market reaction. *Journal of Hospitality and Tourism Technology*, *11*(2), 277–290. **doi:10.1108/JHTT-05-2019-0080**

Arora, A., & Mendhekar, A. (2021). Innovative techniques for student engagement in cybersecurity education. In *Data Management, Analytics and Innovation* (pp. 395–406). Singapore: Springer. **doi:10.1007/978-981-15-5616-6_28**

Blackwood-Brown, C., Levy, Y., & D'Arcy, J. (2021). Cybersecurity awareness and skills of senior citizens: A motivation perspective. *Journal of Computer Information Systems*, *61*(3), 1–12. **doi:10.1080/08874417.2019.1579076**

Cabaj, K., Domingos, D., Kotulski, Z., & Respício, A. (2018). Cybersecurity education: Evolution of the discipline and analysis of master programs. *Computers & Security*, *75*, 24–35. **doi:10.1016/j.cose.2018.01.015**

Cassotta, S., & Sidortsov, R. (2019). Sustainable cybersecurity? Rethinking approaches to protecting energy infrastructure in the European High North. *Energy Research & Social Science*, *51*, 129–133. **doi:10.1016/j.erss.2019.01.003**

Corradini, I., & Nardelli, E. (2020). Developing digital awareness at school: a fundamental step for cybersecurity education. In *International Conference on Applied Human Factors and Ergonomics* (pp. 102–110). Cham: Springer. **doi:10.1007/978-3-030-52581-1_14**

Crumpler, W., & Lewis, J.A. (2019). *Cybersecurity Workforce Gap*. Center for Strategic and International Studies (CSIS).

Cybint. (2020). *Alarming Cyber Security Facts and Stats*. Retrieved from https://www.cybintsolutions.com/cyber-security-facts-stats

Dahbur, K., Bashabsheh, Z., & Bashabsheh, D. (2017). Assessment of security awareness: A qualitative and quantitative study. *International Management Review*, *13*(1), 37.

Demmese, F., Yuan, X., & Dicheva, D. (2020). Evaluating the effectiveness of gamification on students' performance in a cybersecurity course. *Journal of the Colloquium for Information Systems Security Education*, *8*(1), 6–6.

Gartner. (2020). *Forecast Analysis: Information Security, Worldwide, 2Q18 Update*. Retrieved from https://www.gartner.com/en/documents/3889055

Gonzalez, H., Llamas, R., & Ordaz, F. (2017). Cybersecurity teaching through gamification: Aligning training resources to our syllabus. *Research in Computing Science*, *146*, 35–43.

Harris, M.A. (2015). Using Bloom's and Webb's taxonomies to integrate emerging cybersecurity topics into a computing curriculum. *Journal of Information Systems Education*, *26*(3), 219–234. Retrieved from https://aisel.aisnet.org/jise/vol26/iss3/4

Imgraben, J., Engelbrecht, A., & Choo, K.K.R. (2014). Always connected, but are smart mobile users getting more security savvy? A survey of smart mobile device users. *Behaviour & Information Technology*, *33*(12), 1347–1360. **doi:10.1080/0144929X.2014.934286**

Jin, G., Tu, M., Kim, T.H., Heffron, J., & White, J. (2018). Evaluation of game-based learning in cybersecurity education for high school students. *Journal of Education and Learning (EduLearn)*, *12*(1), 150–158. **doi:10.11591/edulearn.v12i1.7736**

Jorgensen, R., Rowe, D., & Wyler, N. (2017). Competitions and gamification in cybersecurity education and workforce development and evaluation of real world skills. *Journal of Computing Sciences in Colleges*, *33*(2), 155–156.

Kreider, C., & Almalag, M. (2019). A framework for cybersecurity gap analysis in higher education. Retrieved from https://aisel.aisnet.org/cgi/viewcontent.cgi?article=1005&context=sais2019

McCrohan, K.F., Engel, K., & Harvey, J.W. (2010). Influence of awareness and training on cyber security. *Journal of Internet Commerce*, *9*(1), 23–41. **doi:10.1080/15332861.2010.487415**

Ministry of Digital Affairs. (2017). *The Strategy of Cybersecurity of the Republic of Poland for the years 2017–2022*. Retrieved from https://www.gov.pl/web/cyfryzacja/strategia-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022

Ministry of National Education. (2017). *Cybersecurity in schools*. Retrieved from https://men.gov.pl/ministerstwo/informacje/cyberbezpieczenstwo-w-szkolach-list-minister-edukacji-narodowej.html

Newhouse, W., Keith, S., Scribner, B., & Witte, G. (2017). National initiative for cybersecurity education (NICE) cybersecurity workforce framework. NIST special publication, *800*(2017), 181. **doi:10.6028/NIST.SP.800-181**

Pawlowski, S.D., & Jung, Y. (2015). Social representations of cybersecurity by university students and implications for instructional design. *Journal of Information Systems Education*, *26*(4), 281–294. Retrieved from https://aisel.aisnet.org/jise/vol26/iss4/3

Pencheva, D., Hallett, J., & Rashid, A. (2020). Bringing cyber to school: Integrating cybersecurity into secondary school education. *IEEE Security & Privacy*, *18*(2), 68–74. **doi:10.1109/MSEC.2020.2969409**

Pendley, J.A. (2018). Finance and accounting professionals and cybersecurity awareness. *Journal of Corporate Accounting & Finance*, *29*(1), 53–58. **doi:10.1002/jcaf.22291**

Rahman, A., Malaysia, N.A., Sairi, M.T.U.K., Zizi, I.K., & Khalid, F. (2020). The importance of cybersecurity education in school. *International Journal of Information and Education Technology*, *10*(5), 378–382. **doi:10.18178/ijiet.2020.10.5.1393**

Ros, S., Gonzalez, S., Robles, A., Tobarra, L.L., Caminero, A., & Cano, J. (2020). Analyzing students' self-perception of success and learning effectiveness using gamification in an online cybersecurity course. *IEEE Access*, *8*, 97718–97728. **doi:10.1109/ACCESS.2020.2996361**

Siddiqui, Z., & Zeeshan, N. (2020). A survey on cybersecurity challenges and awareness for children of all ages. In *2020 International Conference on Computing, Electronics & Communications Engineering (ICCECE) IEEE*, 131–136. **doi:10.1109/iCCECE49321.2020.9231229**

Son, J., Bhuse, V., Othmane, L.B., & Lilien, L. (2015). Incorporating lab experience into computer security courses: three case studies. *Global Journal of Enterprise Information System*, *7*(2), 69–80.

Tirumala, S.S., Valluri, M.R., & Babu, G.A. (2019). A survey on cybersecurity awareness concerns, practices and conceptual measures. In *2019 International Conference on Computer Communication and Informatics (ICCCI), IEEE*, 1–6. **doi:10.1109/ICCCI.2019.8821951**

Venkatachary, S.K., Prasad, J., & Samikannu, R. (2018). Cybersecurity and cyber terrorism-in energy sector – a review. *Journal of Cyber Security Technology*, *2*(3–4), 111–130. **doi:10.1080/23742917.2018.1518057**

Whitty, M., Doodson, J., Creese, S., & Hodges, D. (2015). Individual differences in cyber security behaviors: an examination of who is sharing passwords. *Cyberpsychology, Behavior, and Social Networking*, *18*(1), 3–7. **doi:10.1089/cyber.2014.0179**

Zhang-Kennedy, L., & Chiasson, S. (2021). A systematic review of multimedia tools for cybersecurity awareness and education. *ACM Computing Surveys (CSUR)*, *54*(1), 1–39. **doi:10.1145/3427920**

Zwilling, M., Klien, G., Lesjak, D., Wiechetek, Ł., Cetin, F., & Basim, H.N. (2020). Cyber security awareness, knowledge and behavior: A comparative study. *Journal of Computer Information Systems*, 1–16. **doi:10.1080/08874417.2020.1712269**