Judit Takács MÓDNÉ

The importance and development of safety awareness with soft skills in industrial environments

The 21st-century living space

In the 21st century, cyberspace has become our lives' scene. Many people work, study, shop, meet, communicate through the World Wide Web. The range of applications is almost endless. From a very young age, we meet the world wide web, all we must do is turn on the television and watch a movie. In addition, there are other effects of this shift in living space. In the 21st century, the young generation is socialized in cyberspace. It affected and meaningfully changed people's personal and work relationships, the nature of their relationships, and the development of their soft skills.

Companies and individuals may think that they are too small and unlikely to be attacked. They believe their systems are well-armed and well-defended, so they do not expect an attack. Unfortunately, the cases of countless Hungarian factories in recent years also provide enough warning examples to deal with the protection of our systems. Often, IT security incidents are due to the company's infrastructure and operational deficiencies. "Users' security awareness is the first line of defence, not the firewall." It is necessary to take the security awareness attitude of employees. And not only knowledge but compliance with the rules is relevant. It is a great way to reduce potential attacks chances of success. (Bóna, 2020)

Thus, the expectations and needs of the labour market constantly change, with the modified environmental impacts, cybersecurity threats and generational characteristics of employees. (Kollár & Poór, 2018)

In this empirical research, the goals are to apply our knowledge in practice and its relationship correlation. In the hypothesis, the development of soft skills positively affects security awareness and expected competencies in today's job market. Additionally, cybersecurity as a competency has grown into a 21st-century, essential, scalable skill.

The literature review of terms related to safety, security awareness, and soft skills

This paper revises and systematizes the 21st-century skills presented in the introduction and related concepts such as cybersecurity attitude, knowledge and awareness, soft skills by summarizing the relevant literature. The study maps out the connections between each concept according to the current state of the science. Why is it essential to focus on cybersecurity today? What is the exact difference between knowledge and awareness? How can we most places the acquired knowledge at a conscious level? What indicators are available in measuring various soft skills and security awareness attitudes? How can these skills be developed? The author reviewed the following concepts in sync with the research from different approaches and their connections.

The importance of information security and cybersecurity in today's society

The benefit of the online world is that it facilitates the acquisition of data and information (Fregan, Kocsis & Rajnai, 2018). Cloud-based services make data and operations available from anywhere in the world. However, there are many downsides to this, as it carries countless dangers. An inadequately protected set of information circulating online is available to anyone at any time. The focus should be on examining the issue, who seeks and uses them for what purposes.

Cyber awareness, security awareness has developed into an essential and expected attitude since the advent of the digital age. Everyone should treat security awareness behaviour as a priority from an

economic, social, and governmental point of view (Nyikes, 2017). The presence of security awareness is becoming significant in today's world and is, thus, central to higher education (Novák, 2018).

Cybersecurity education focuses on developing online competencies and skills to participate effectively in the online world. It includes all kinds of awareness, knowledge, attitudes, skills, and participation required for a platform in different cyberspace. It requires cooperative consideration of technical and behavioural aspects. (Santhosh & Thiyagu, 2019)

Knowledge and awareness in the light of security

As Freud said, "Consciousness was only the tip of the iceberg, and the underwater part of the iceberg is the centre of gravity from which the motives come." He later thought about this with Jung, and they concluded that "if one becomes more aware of the subsurface layers within oneself, one will fail in lifeless." (Butler-Bowdown, 2007)

When looking at the safety aspect of this statement, it is essential to target this awareness process primarily. In this process, we even aim for a lifelong learning and knowledge acquisition process. In this process, everyone needs to achieve awareness with sufficient motivation, interest, and practice.

"Introduction of new forms of training, including the lifelong learning model; open and online training; education in collaboration with education and business" (Fregan, Kocsis & Rajnai, 2018). Of course, educational institutions also have a fundamental role to play in acquiring knowledge. First, we must consider the peculiarities of the generation and the fact that the Z and alpha generations can already be considered a kind of digital native. Then we have to deal with the appropriate training from primary school onwards, as with the continuous development of technology, knowledge changes.

According to some studies, the lack of knowledge is not the problem, but they are not applied or realized in real life (Szarvák & Póser, 2020). According to other studies, a survey in Hungary (managers with more than 400 employees) shows that very few have sufficient information security awareness and knowledge (Kollár & Poór, 2019).

As prevention is paramount in terms of security awareness, as it is in all areas of life (health, protection of our homes, transport), "in terms of cybersecurity, the security awareness of the individual must be increased to prevent avoidable incidents." (Nyikes, 2017)

Security awareness and soft skills in today's job market

Daniel Goleman (1995) "What do employers want?" based on its survey (involving 120 companies), they were asked to list the qualities that make their best employees stand out. Based on the results, the world of work and expectations have changed. It is no longer the professional knowledge, the practice that may be the quotient of the individual's intelligence is decisive, but the individual's soft skills have come to the fore. Goleman's list was "listening and communication skills, the ability to adapt to change and overcome difficulties, confidence, motivation, career-building intent, cooperation and conflict management skills, participatory or leadership ambitions.". (Butler-Bowdown, 2007)

21st-century labour market expectations and knowledge of available workers do not match. There is a significant gap between expectations and the knowledge generated during their training (Fregan, Kocsis & Rhine, 2018). This finding can be further extended to, for example, cybersecurity competencies due to the generational characteristics mentioned in the previous points and the shift of the world of work to cyberspace. The human factor and the social engineering that focuses on it remain a critical area in information security. Generation Z workers have a different set of values, working differently. Their experience has shown that the rules are more difficult to be tolerated and hard to integrate. They are predominantly striving for self-realization. It makes it hard to work in a team and to put the interests of companies first. Its positive fact is that "because they know and use the latest digital devices, techniques, applications and services with confidence, they do not have any difficulty in teleworking, in understanding teleworking processes, in actively participating in them" (Kollár & Poór, 2018).

Despite the age of digital indigenousness, "our security awareness and defence reflexes have not yet developed as they have ensured man's survival for thousands of years in physical space, evolutionary development." (Nyikes, 2017)

"Many people are looking for protection against threats in more advanced technical solutions. The more alarms we have, the more secure we feel." (Butler-Bowdown, 2007). This view focuses specifically on external security tools, technology control. There is no need for employee training, awareness, continuous control, or the application of the limitations achieved by technology.

According to the other point of view, "even the application of the most effective defence technology is not worth much if people do not act consciously and do it to a high degree." (Nyikes 2017). The most effective protection technique is prevention. As we know, human is the weakest link in this process. The employee must have appropriate professional knowledge, be trained, be motivated, and be able to develop his or her skills and be able to put the knowledge into practice. In addition, the development of safety awareness is determined not only by expertise and learning but also by motivation, emotions, behaviour, culture, interest (Szarvák & Póser, 2020). With this knowledge, the question arises that if we combine security awareness with appropriate security skills, complemented by relevant security skills, can we help to get the right cybersecurity competencies?

The purpose of the research, research questions, and research method

After reviewing the literature, the 21st-century employers' experience has examined in practice what skills they need, what methods they used to measure the skills inspected, and whether they pay due attention to their development. The research aims to map industry participants' significant expectations and needs, with a particular focus on soft skills and safety awareness. Through the research questions, what methods companies used to develop their employees' skills have been surveyed. The acquired/used knowledge measures, awareness, and the best measuring practices were reviewed. Furthermore, the research looks for the relationship between how the development of individual skills affects the development of cybersecurity competencies. There is a connection between the development of awareness and the development of different skills.

These responses were compared to examine how well companies can apply the practical, innovative methods suggested by the experts. After these, the main question is to what extent can public and higher education support the needs of the labour market by developing students' skills based on their experience? The following research questions and topics were formulated:

- What cybersecurity knowledge, skills, soft skills should a 21st-century employee have at your company? Can you list the most relevant skills you need?
- What do you think are the primary skills to be developed among recent graduates and young workers?
- Are there relevant work areas and workgroups in terms of information security risk at your company? How is it different for these groups to develop safety awareness skills, and how are the expectations for employee skills divergent?
- How significant are the expectations related to information security and cybersecurity awareness at the company?
- How is safety awareness measured and maintained? How do they ensure and compensate for the lack of skills and knowledge?
- How often is training used to develop safety awareness? What type of surveys do they prefer? (Online, personal training or online tests)
- What soft skills can help develop a safety awareness attitude and be effective? Do they also pay attention to developing these soft skills?

In this research, a mixed-type, empirical, qualitative research method over personal interviews was used among the Dual Partner Companies of the Alba Regia Faculty of Engineering of the University of

Óbuda. There are many advantages of structured and in-depth interviews. For example, we can collect comparable answers during the conversation with a predefined set of questions. Furthermore, it helps to express a free opinion while raising new directions concerning the research topic.

This research is a pre-survey, preliminary exploration. Nevertheless, the result contributes to the solution of a practice-oriented problem aimed at a productive method of developing safety awareness and increasing the efficiency of measurement by integrating it into the educational process. Educational processes need to change, as they need to follow 21st-century industrial soft skill expectations and the particularities of Z (current workers) and Alpha (future workers) young people.

Participants in the study

Based on the literature research, a significant proportion of corporate participants are under-informed about the new information security challenges. All companies have data protection and information security regulations. These are usually checked once a year in the form of a test, but each participant usually experiences assessment forms as a necessary inconvenience. Respectively, employers interpret it as an obligatory element, which is enough to tick and do, so they do not focus the development just on its performance. "The increasing number of hacker attacks on companies indicates that information security needs significantly more and more serious than before.". (Kollár & Poór, 2018)

The sampling took place at eight multinational companies participating in the dual training of the University of Óbuda. They have been employing dual students for years, so they are experienced in the new generation of workers. Therefore, they already have enough experience with young workers who are still in or just out of the education system. Respondents requested their anonymity for security reasons, so the study refers to them as A1 ... A8. At some companies, it had the opportunity to ask several experts on the research topic. During the conversations, besides the general security measures of the companies, their information security and cybersecurity training and measurements were examined. The multinational companies surveyed belong to different industrial sectors. For each company, the issue of cybersecurity has become a part of their lives. It has been amplified and made necessary not only by digital development but also by the pandemic.

Introduction of research results

Interviews have surveyed with various executives or professionals who care about security processes at companies. During the discussions, valuable feedback, thought-provoking information was gathered, which will also facilitate further research. The results of the answers to the questions presented in the previous chapter are presented below.

The expectations of 21st-century employers in terms of safety awareness and soft skills

The cybersecurity knowledge, skills and soft skills of the interviewed companies show a rather diverse picture in the practice of 21st-century employees. Let us look at information security expectations first. Because of security risks, in many cases, it is not left to the individual (excluding the human factor) to protect. Usually, a special department deals with managing security rules, detecting and resolving problems. They keep the level of safety awareness up to date with various pieces of training, strongly tied policy and occasional newsletters, and communication. As a result, there is a lower level of safety awareness than direct workers. It is also significant to them, as they operate electronic equipment. Typically, indirect workers have higher expectations of the necessary safety awareness.

Overall, every layer of employees should have a minimal safety awareness attitude. The expectations are consistent with the nature of the work. Then the question is, what counts as minimal knowledge of the security subject? The basic requirements listed were compliance, adaptability, considered correspondence, proper management of each website, sufficient passwords complexity, secure

handling of credit card transactions and other confidential data protection. Of course, these do not exhaust all possible hazards and the minimum protection measures when looking at the individual level of responsibility.

The general knowledge and soft skills expected were very consistent based on the answers. Proper professional knowledge, IQ and EQ are essential. Be flexible and compliant with the employee. Follow the principle of lifelong learning, have the right learning skills, interested in learning continuously and develop, have the right intrinsic motivation. Several respondents gave priority to the base competencies, have digital competencies, be able to count, read and interpret texts correctly, not only in their native language but in at least one foreign language.

There is more and more project work at companies. Employees necessary needs are capable of Teamwork, collaboration skills, conflict management skills and stress tolerance. Employers expect employees to be proactive. It would be helpful for employees to recognize the potential of situations and not just follow simple instructions. Employees need to be creative enough, and they need critical thinking and problem-solving skills. Communication and presentation are also necessary skills. Adequate flexibility and professionalism are also important.

Table 1.: A summary of the situation of the skills and knowledge required

Expected skills and knowledge	Lack of skills and knowledge
critical, **logical thinking and problem-solving skills**	logical thinking and problem-solving skills
learning skills, intrinsic motivation and desire for development	learning skills
communication and presentation skills	communication and presentation skills
teamwork and cooperation	teamwork
compliance and accountability	compliance and accountability
flexibility and creativity	
stress tolerance and management	stressmanagement
count, read and understand text, **foreign language and digital skills**	foreign language and digital skills
professional experience, knowledge	professional experience, knowledge

After evaluating the lack of skills, this indicates previously listed skills are problematic for employers. Most of the young people who come to them have only partial or no skills at the level that companies expected. Some examples are shared from the interviews below.

- "*Just to give a few examples of the skills of young workers, for example, they cannot write an appropriate style of email or present their work to the team.*" (Interviewee A2)
- "*Professional shortage, universities do not teach professional things at the right level to be able to work with fresh workers right away. At least 3-4 months of training is required after admission.*" (A4 interviewee)

- "*Adherence to basic rules at work is problematic. (such as ignoring the leave request process, avoiding the entry system, or not using it, respecting breaks and working hours) Following the rules and taking responsibility seems to be lacking.*" (A5 interviewee)
- "*They cannot think logically, they have a hard time seeing the connections. They cannot work in a team. Overall, the expected soft skills based on experience are not adequate*." (A6 interviewee)
- "*Perhaps the biggest problem is communication, more specifically the lack of proper communication. Or to use the acquired knowledge in a good place and form.*" (A8 interviewee)

Many can acquire basic skills independently, but some students find it quite complicated to do it alone. Dual training provides plenty of help in bridging the gap in this regard. Students can drop off their mentors during their studies, learn the importance of relevant soft skills, and develop them either alone or with help. (Pogatsnik, 2019)

Areas with high information security need and expectation at the companies surveyed

The interviewed companies listed the relevant work areas and workgroups in terms of information security risk. All respondents highlighted administrative positions, HR, and Finance departments. The IT department is essential everywhere, as they create and operate various protection and security systems. In addition, some companies have a specialized training department that tries to maintain employee awareness and achieve skills development through different repetitive training.

"*There is a department in the company where employees can only enter the workspace with special privileges. These extra privileges are only temporary. They repeatedly renew if the job requires it.*" (A4 interviewee)

Some priority departments have high expectations for employees. Especially in places where employees deal with sensitive data, product prices, product drawings. The following conclusions can be drawn from the responses. First, employers know there is sensitive data. Second, they know that external control does not protect everything, but employee safety awareness is not advanced enough.

"*I would like to highlight the IT sector in the company: it is not enough to create OS layer security or use filesystem-based protection. Nevertheless, if we go even deeper into security levels, a network firewall should protect company data. From an IT point of view, the expectations of individual employers towards employees could be higher.*" (A7 interviewee)

Examining the answers received, the answer to the following question was very thought-provoking. How significant are the expectations related to information security and cybersecurity awareness at the company? The safety awareness expectation is not substantial in practice for companies. Employers seem to be distrustful or pay little attention to employee development. They try to ignore the human factor, and they want to prevent possible attacks with external restrictions.

Tools and methods for measuring safety awareness in companies

To fill and measure the necessary skills gaps, companies hold annual pieces of training for employees. The training is usually online, which in many cases cannot be linked to internal motivation but rather to an external, necessary element of the work process. The training ends with a test, usually in an online form.

There is also ad-hoc information or post-incident information and communication from the company. However, these do not happen everywhere and with unpredictable frequency.

"*If someone does not reach the minimum level, they take part in another training right away, so they have to repeat it until they reach it.*" (A6 interviewee)

Some companies also use knowledge transfer meetings led by IT security. In these discussions, the workers concerned are well informed and given examples of certain shortcomings and how to deal with them.

The tests are easy to perform, the shared content (text, video) is not complicated, anybody can solve it even without serious attention, the minimum level is easy to accomplish.

There are several suggestions and ideas on how to make this process more efficient.

"*They could supplement the tests with possibly hidden questions from which to deduce how the worker would react in a given situation. The employers could check the level of safety awareness skills with questions examining social engineering aspects. Nevertheless, at present, the company is characterized only by simple training and a traditional test.*" (A3 interviewee)

Everywhere they apply a survey of all employees about their skills when entering and hiring a company. These are more about personality, professional issues, and possibly with little security awareness. To increase safety awareness, only annual pieces of training and tests are currently available to the respondent. According to them, this is not enough and is ineffective. Manual workers are usually subject to a paper-based test and personal training, referring to different skill levels and needs.

Soft skills that can help to acquire and apply safety awareness skills more effectively

The research looked for the answers with the interviewees about what kind of soft skills could support the development and maintenance of the security awareness attitude.

"*Discipline, compliance, sobriety, empathy (understanding the company's interests and goals), loyalty can support the development of a security awareness attitude.*" (A4 interviewee)

Many respondents highlighted the ability to work with the team and self-knowledge. After all, if the worker knows himself to enough degree, knows how reliable knowledge reacts to dangerous situations, he can easily prevent them. There are other benefits of self-knowledge. Furthermore, better human knowledge supports several necessary, expected skills like cooperation, communication, conflict management. In many cases, the mistakes of internal workers cause the incidents. If workers have deep human knowledge, they can take preventive action and avoid attacks easily.

Caution, analytical vision, and a high degree of compliance are significant. Companies have security regulations, but their workers do not comply with them.

The study examined whether companies pay attention to the expected soft skills development listed in the previous sections.

Unfortunately, at present, "*the development of these listed missing skills is left to the workers. They need to learn independently, based on articles, based on individual practices. Alternatively, if we have the option in the form of online training.*" (A7 interviewee)

Representatives of the company gave only a few positive answers about the development opportunities. "Some leadership skills development, conflict management skills development, or teamwork training has been launched." (A5 interviewee) The reason why is no more, not revealed. It may be of a financial origin, or its culture has not yet developed in companies. These attitudes need to change, skills need to be developed, and education needs to prepare future employees for these needs.

Sharing good practices, good experiences that are effective in maintaining awareness

The leaders of the companies had some ideas, suggestions, good practices that can be useful in the future to acquire the appropriate level of safety awareness and necessary skills.

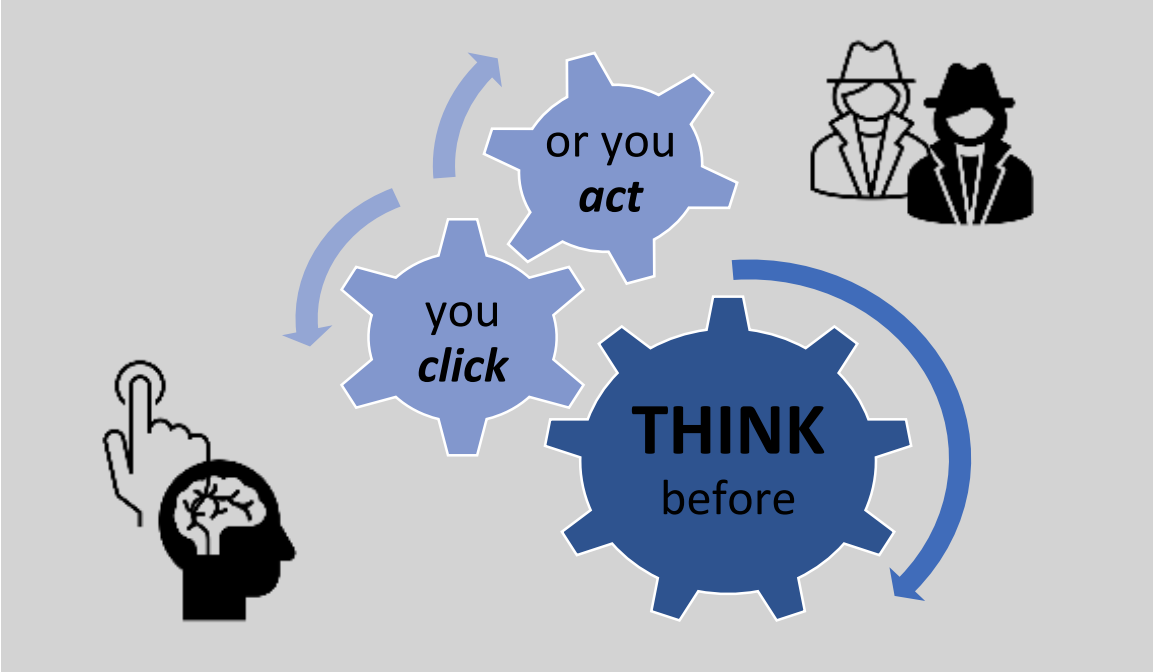
Employees who have access to sensitive data at work would require serious monitoring upon hiring. The job interview usually includes professional questions and IQ-related questions with logic and foreign language tests. Greater attention should be paid to tests of soft skills and personality traits in multiple jobs, complemented by cybersecurity competencies. It is needed mainly in jobs with sensitive data, but the study found the non-existence of hardly any jobs where this would not be emphatically important. It is consequently easier to assess and predict the employee's response to future critical situations. Employers should examine stress tolerance, collaboration, and conflict management skills. These surveys should be repeated not only at the time of admission but at intervals. Depending on the result, obtain developer training. Self-knowledge tests could be solved periodically, in a developmental way, and evaluated with the help of a professional. However, it would result in many lost working time and more resources that are not available for many corporations. Companies would need effective methods that are not currently available or do not work effectively.

"*The cybersecurity expectation must work top to bottom. In cybersecurity, we need to define what value means to the company. "Threats to corporate values need to be considered. They have to identify the manner of threats and the people involved. Communication has a big role to play within companies. Every employee needs to be constantly aware of what attacks to expect. Companies could build development training on knowledge and communication. Of course, a lot depends on attitude. Above all, control is needful to play a supervisory role.*" (A3 interviewee)

In addition to critical and analytical thinking, employers need to explain to their employees the importance of social engineering in today's world.

"*The motto of our company is also the motto of the press release issued by The European Union Agency for Cybersecurity (ENISA), slightly rewritten: "**Think before you click - or you act**"* (A7 interviewee)

Figure 1.*:* "Think before you click - or you act" - to be followed by everyone



It should be the motto for summarizing the results. 21st-century companies and the education system do not pay enough attention to the human aspect of the necessary security threats and the required soft skills development. We know and are aware of many dangers, but knowledge is unfortunately not enough in today's digital world. Unfortunately, the knowledge and skills required, plenty of workers fall short of expectations, if not decades. Regulations are often not read. Even if they read it, they do not follow. There is a clear need to introduce reforms in education, training, development, and testing that are more effective in supporting the interests of companies.

Summary, conclusion, and future work

Considering the expectations of the 21st century, the skills and competencies of the previous years are no longer enough. Therefore, thousands of research, results and suggestions have been made on the topic in recent years.

Unfortunately, in practice, this issue is still problematic from a human point of view. Isn't it because of the proper methods? Because of inadequate motivation? Not good measuring tools? Why can't companies appropriately protect their data with advanced IT backing? Many questions remain unanswered.

Till technology is evolving, people are changing, our tools and methods are becoming obsolete. In the future, the community will need new, strong competencies. Security awareness should not be a necessary lousy task in the workflow. Security topics will be a routine task in which it is in the interest of all parties to strengthen the line of defence. As participants have changed, technology is constantly evolving, cyberspace has become commonplace, so this will require a focus on new methods to help strengthen cyber competence in the future.

Cyber competence can replace digital competence, which requires more complex and diverse skills and attitudes. In addition, another correlation can be seen in this process. The lack of soft skills, not only as a lack of relevant competencies in employment but also in terms of the role of human factors, can in many cases increase information security risk factors in cyberspace.

In addition to external control methods, prevention has a significant role to play in increasing efficiency. These, in turn, need to be rethought in the light of the specificities of the new generation. New methods, a new motivational system and proper communication are necessary. It is relevant to make employees interested in the present and the future. Facilitating this is the future task of education and companies. Educational institutions can prepare forthcoming employees by imparting the proper knowledge and strengthening students' skills. Companies can keep the skills they need up to date with suitable methods.

All industry organizations need to pay close attention to the importance of protection when designing new systems. The designing process requires IT professionals with appropriate cybersecurity skills. Education must also play a dominant role in this. Collaboration between business leaders, industry, professionals, employers, employees, and education needs to be even closer. They can identify and serve extreme rapidly changing needs.

Companies need to build a new kind of protection system to support the protection of cloud-based workflows. Security technology is paramount in any new system design, as there is no longer any data that would not be uploaded to the World Wide Web in some form at all times. They have to develop new training methods and systems considering different skills, ages and generational characteristics. The technique of measuring competence and improving a safety awareness attitude needs to be changed.

The future directions of the research are to support these methods and measurement tools. It requires a deeper examination of current techniques, measurement tools and their effects on workers. Special attention will be paid to examining the motivational routines of the Z and Alpha generations in the future. A reform of the methods used in the industry could be proposed.

References

- Butler-Bowdown. (2007). *Pszichológia dióhéjban 50 pszichológiai alapmű.* (Psychology in a nutshell 50 basic works of psychology) HVG Kiadó Zrt. Budapest.
- Fregan, B., Kocsis, I., & Rajnai, Z. (2018). Az IPAR 4.0 és a digitalizáció kockázatai. (Risks of IPAR 4.0 and digitization) *Műszaki Tudományos Közlemények*, *9*(1), 87–90. https://doi.org/10.33895/mtk-2018.09.17
- Kollár, C., & Poór, J. (2018). Szervezetek a digitális korban – A digitális munkahely információbiztonsági aspektusa. (Organizations in the Digital Age - The Information Security

Aspect of the Digital Workplace.) *Kiberbiztonság – Cyber Security,* Tanulmánykötet a Biztonságtudományi Doktori Iskola Kutatásaiból Budapest, Magyarország : Óbudai Egyetem, Bánki Donát Gépész és Biztonságtechnikai Mérnöki Kar, 95–107.

- Novák, J. (2018). Biztonságtudatosság növelésének eszközei a felsőoktatásban. (Tools for raising safety awareness in higher education.) *Műszaki Tudományos Közlemények*, *9*(1), 183–186. https://doi.org/10.33895/mtk-2018.09.41
- Nyikes, Z. (2017). A biztonságtudatosság fejlesztésének egyes lehetőségei. (Some options for developing security awareness.) *Műszaki Tudományos Közlemények*, *7*, 327–330. https://doi.org/10.33895/mtk-2017.07.74
- Péter B. (2020). *A felhasználók biztonságtudatossága az első védelmi vonal* (User safety awareness is the first line of defense) – *Videó*. https://bit.ly/3lKeqG7 *(last viewed 2021.07.01)*
- Pogatsnik, M. (2019). Measuring Problem Solving Skills of Informatics and Engineering Students. IEEE 19th International Symposium on Computational Intelligence and Informatics and 7th IEEE International Conference on Recent Achievements in Mechatronics, Automation, Computer Sciences and Robotics (CINTI-MACRo*)*, Szeged, Hungary, 93-98, doi: 10.1109/CINTI-MACRo49179.2019.9105277.
- Szarvák, A., & Póser, V. (2020*). Information Technology Safety Awareness – a review of regularly used terms and methods.* 15th International Symposium on Applied Informatics and Related Areas Organized in the Frame of Hungarian Science Festival 2020: AIS Székesfehérvár, Magyarország: *Óbudai Egyetem*, 107–111.
- Thiyagu, K., & Santhosh, T. (2019). *Cyber safety and security education*. Lulu Publication.