EDUCATION IN CYBERSECURITY

Rodica Bulai, Dinu Țurcanu and Dumitru Ciorbă[1]

DOI: 10.24989/ocg.v335.2

Abstract
The article addresses education as the smartest investment in cybersecurity. One of the most intriguing findings is that 95% of security incidents involve human errors. Most security attacks are concerned with human weakness to attract victims and persuade them to give involuntary access to personal and sensitive information. To eliminate errors caused by social engineering and negligence and to increase users' awareness of the threats, technologies and services should be combined with education. Education in the field of cybersecurity is a necessary consideration for both individuals and families, as well as for businesses, governments and educational institutions.

For families and parents, the online safety of children is of major importance. Equally essential is the protection of information that might affect your personal finances, and precious family assets, such as photos, videos etc.

For educational institutions, it is important to understand the link between the online world and the "real" one. Teachers, staff, students, tutors, pupils, etc. should be trained in appropriate on-line behavior to reduce vulnerabilities and create a safer online environment.

A better awareness through security education can help enterprises protect their intellectual property and ensure availability of services.

Governments hold an enormous amount of personal data and records of their citizens, as well as confidential government information, which most often serves as a target for attack. Only through education and awareness, the confidence in public services can be gained. Cybersecurity depends on education.

1. Introduction

We are facing an eyebrow-raising talent shortfall in cybersecurity. The cybersecurity job market, according to a joint report by Frost&Sullivan and (ISC)2, will see a labor shortage exceeding 1,5 million unfilled positions by 2020 [1]. Given the rapid and continuous evolution of threats, it is critical that educational cybersecurity programs share best practices and curriculum updates.

But it is just as important for enterprises — from startup businesses to large corporations, and from small nonprofits to vast government agencies — to do their part. They have the means as well as the critical need to enhance their employees' cybersecurity knowledge.

[1]Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics, Str. Studentilor 7, Chisinau, MD-2012, Republic of Moldova, Tel:(37322) 509908; E-mail:rodica.bulai@ati.utm.md, dinu.turcanu@adm.utm.md, dumitru.ciorba@ati.utm.md

Even those employees who did arrive with security knowledge have more to learn. The field of cybersecurity is constantly expanding, with more domains to secure and more ways to attack. Intrusions are harder to detect; attackers are stealthier and more evasive.

The best defense is to provide comprehensive education programs for all. You don't have to turn everyone into a cybersecurity expert. IBM, for example, requires all employees to complete digital training each year, which covers matters from secure handling of client data to appropriate sharing on social media sites. Employees can easily learn how to spot and avoid the most frequent types of threats, such as phishing attacks in emails.

Whether taught in a school, university setting or carried out in an enterprise, cybersecurity is a holistic problem and needs a holistic solution. Just as educational institutions start to develop interdisciplinary approaches (such as joint programs between computer science and business, medical, law, economics, public policy, criminology, and even journalism schools), organizations should ensure that their approach to security reaches the people responsible for infrastructure, human resources, data, applications, ethics assurance, management policy, and legal compliance.

There have been technological advancements within the last few years to help secure corporate networks against unintentional, or intentional, risky behavior by users. But while such technical controls and the establishment of sound policies are essential components of effective security, educating, in cybersecurity is one of the best investments a country can make — and a rational recognition that it will take all of us to create a more secure future[2].

2. The initial period - school - acquaintance with the aspects of cybersecurity and safe "surfing" in a virtual environment

The peculiarity of the socio-economic development of the Moldovan economy, and of the world economy as a whole, determines the presence of a significant number of risks, including informational ones, which pose a threat to the stable functioning of any enterprise and person.

These aspects require the formation of an "informational" culture, which should be cultivated in every person, starting from school. These will then develop in the course of evolution at the university and at the workplace. All these steps, in our view, must comply with certain requirements/standards, and with three pillars – three qualities:

a) to study – to explore – to know;

b) to teach – to accustom – to be able;

c) responsibility – consciousness – implication.

So, in school/ lyceum we consider it is necessary to develop and to implement in the following areas: the study of awareness of students about staying safe while surfing the Internet; the familiarization with the rules of safe work on the Internet; the formation of students' informational culture, the ability to independently find the necessary information using web-resources; the discipline training while working on the network.

The trainees should know: the list of the Internet information services; the rules of the safe work on the Internet; and the danger of a global computer network.

The trainees should be able to: responsibly treat the use of on-line technologies; work with web-browser; use information resources; search for information on the Internet.

A good start for the Republic of Moldova is that on June 14, 2018 the Memorandum of Understanding on the development of digital education in general education was signed, and as a result of this agreement the curriculum, the electronic support and the Guide for Students and Teachers of the 1st grade were developed; the virtual library, www.smartedu.md, was consolidated; funds have been collected for the procurement of 1850 digital tablets in support of each Ist grade teacher across the country. In the 2018-2019 academic year, the "Digital Education" module will be studied by 34,642 students, being compulsory for the 1st grade pupils and optional for those of II - VI grades. In this respect, it is important that Digital Education also develops cybersecurity culture. Analyzing the primary, secondary and lyceum curricula for Informatics, compulsory or optional, we only met in the updated curriculum for the VIIth grade - HOW TO BEHAVE IN THE VIRTUAL SPACE. In this regard, we consider that cybersecurity education modules must be included in every curriculum of Informatics for all the grades from the Ist to the XIIth.

The International Center for Protection and Promotion of Women's Rights "La Strada" of the Republic of Moldova undertook a series of actions to create information services for both children and parents/teachers (portal www.siguronline.md). The portal provides young users with the opportunity to access useful information about how to protect themselves from abusive content and actions in the virtual environment, how to develop a responsible attitude to the posted content, and to report possible abuse, while retaining anonymity. The General Prosecutor Office has set up a hotline where virtual crimes can be reported. The Police General Inspectorate has been involved in a number of projects such as, *Together we make the Internet better* !, *An informed child - A protected child* for the protection of children's rights and needs in the Republic of Moldova. We come to realize that we all have a common responsibility to make cyber space safer for everyone, especially for children, namely through information, education and awareness.

3. The transit period - the university - the study and development of the principles and standards to ensure and respect for cybersecurity

Methods and cybersecurity technologies - is the youngest area of IT in our country. The other areas – software, hardware, service – to the contrary, have roots in the “inherited” technologies that were formed several decades ago.

Education of cybersecurity can be divided in two directions: the first is future civil servants, whose activities are not focused on the direct provision of cybersecurity, and the second is training future officials, whose activities are directly focused on the provision and supervision of cybersecurity.

When forming the list of competencies, various formal sources of requirements that employers can present to cybersecurity specialists were analyzed: legislatively approved qualification requirements of the Republic of Moldova state institutions; requirements for civil servants working in the field of cybersecurity; recently appeared professional standards in the field of IT and IS; various international standards for the protection of information, from which you can learn a lot of valuable information about what different levels specialists should be able to do; regulatory documents existing at enterprises describing the functional responsibilities of such specialists, etc.

Education in the field of cybersecurity, in addition to methods and technologies for protecting information resources, always includes the study of means of attack too.

Mass issues on the specialties of the cybersecurity group appeared recently, and only now, the effectiveness of their preparation can be analyzed.

The peculiarity of cybersecurity as an educational subject is that it must combine knowledge in the field of natural sciences and technology, as well as in law, management, a number of humanities, therefore, in addition to courses on methods and means of data protection, fundamental mathematical disciplines, advanced IT training, and the study of organizational and legal aspects of ensuring cybersecurity should be included in the limited scope of the curriculum.

The complex of technical disciplines for students of the cybersecurity is also optimized – they study various aspects of cybersecurity in the physical environment and the features of the organization of this environment itself, mastering the theory and practice of building computing systems. In addition, graduates of this specialty should be able to solve all organizational issues of cybersecurity, which is also dedicated to a separate discipline.

Also, between July 10 and October 31, 2017, a survey was conducted to identify the target professions and training needs in the field of IT security in Moldova. The questionnaire containing 23 questions was completed by 199 companies (the only case in the Moldovan practice when a questionnaire in the field was completed by such a large number of enterprises), IT companies, the provider-companies of electronic communication services and banks, which demonstrates an increased interest from companies in the field of cybersecurity.

Based on this survey, in the recent years, at the Technical University of Moldova, the State University of Moldova, the Academy of Economic Studies of Moldova, and Alecu Russo State University of Balti new learning programs in cybersecurity are emerging.

For the design and development of lycense and master programs in Cybersecurity, also, an analysis of European curriculum documents has been carried out: European Agency for Network and Information Security (ENISA) - Cyber Security Education, National Institute of Standards and Technology (NIST) for Cybersecurity Education (NICE), Information Systems Security Association (ISSA), Information Systems Audit and Control Association (ISACA), Toward Curricular Guidelines for Cybersecurity (ACM), IEEE Computer Society, etc.

At these universities is conducted the targeted training of specialists for the Central Bank, the Ministry of Internal Affairs, and other state institutions of the Republic of Moldova. This approach has a number of advantages. The organization, recruiting graduates who actively collaborated during the last years of training with the university, receives not only the necessary specialist but also a person whom they already know from both professional and moral points of view, which is important for working in the field of cybersecurity. On the other hand, specialists of enterprises with whom the faculty cooperates, actively participate in the educational process, and this involvement of practitioners in teaching allows maintaining the relevance of the courses.

Now there is a technical-scientific center at the Technical University of Moldova. In fact, it has also become the center of crystallization of educational processes on cybersecurity – teaching experience is spread through it, advanced data protection technologies being actively developed and introduced into the educational process.

Today, this center is gradually turning into a mini techno park that teaches students and provides various services in the field of cybersecurity, solving quite complex tasks in the development of new protection methods for the state or commercial enterprises.

Such a synthesis of business and education allows the university independently to earn money to improve its educational process, attract highly qualified specialists to teach and improve the professional level of its employees.

For higher professional education in the field of cybersecurity, the cooperation with companies, which are developing data protection tools, is vital. For universities, such cooperation is not only an opportunity to get modern equipment and software, but also a way to make students feel the pulse of the industry. For market participants, it is an opportunity to influence the university environment, to help universities prepare really necessary industry specialists. Therefore, university professors and practical workers from the company, highly appreciate the level of theoretical training of specialists in the field of cybersecurity in universities, but note its insufficiency from the practical point of view. The main difficulty that university graduates face in finding employment is the lack of skills in the applied use of their knowledge. According to both teachers and practitioners, close cooperation with companies makes it possible to remedy this situation.

The main objectives of such cooperation programs are: the dissemination of advanced knowledge and experience into the field of information protection from modern computer threats; the support of the most talented students interested in studying cybersecurity issues; teachers' training in the field of cybersecurity, as well as the formation of a platform for the exchange of teaching experience with colleagues; providing affordable antivirus protection for higher education institutions, centers of advanced training and retraining of teachers.

Therefore, we believe that the effect brings only an integrated approach to the implementation of the program, which involves a combination of its three main elements: training, research activities and practice. The university partners "Bitdefender", "Endava", "Academia Cisco" provide free training courses, teaching materials, analytical and statistical data, research and reviews of the company leading experts on computer and cybersecurity. Distance seminars are held for teachers and students, master classes and meetings with experts are organized. Under the guidance of experts, students write graduation projects on topics proposed by the company, prepare analytical reviews and articles. Leading experts review all these materials, and the results of the most interesting student studies are applied in the work of the company.

The second line of study at the faculty is cybersecurity aspect of future students whose activities are not focused on the direct provision of cybersecurity. In this case, we consider the method of using the educational-research cryptographic system at the State Engineering University of Armenia, a success [3]. In this respect, TUM initiated a project to develop the Security e-Learning Platform, a teaching-learning tool, individual and distance learning, research and demonstration of real-world security solutions based on case studies. For the start, 5 modules are provided : Criminal Investigation Forensic, Malware Analysis, Reverse Engineering, Clean Code and Capture the Flag (CTF Competition with Various Security Exercises). Such an approach can be used not only by cybersecurity teachers and students, but also by those who do not have a professional background in the field, but intend to study this area whether they are interested in increasing their security skills or to better understand security issues.

With the development of information technologies and the growth rate of their implementation in all socially significant spheres of the society, the problems of information protection become more substantial, which determined the emergence of specialties related to information protection in the list of areas for training specialists in most technical universities. However, knowing the basics of cybersecurity is necessary for almost every user of electronic means of processing and exchanging information. In essence, cybersecurity tends to turn into "third literacy" along with "second literacy" – computer skills and information technology.

To summarize it all we can conclude that the university education in cybersecurity (mostly higher) is not without flaws. According to some representatives of the state institutions, modern education does not meet modern challenges of cybersecurity; graduates are good in physics, mathematics, crypto algorithms, but cannot name the attack vector, the penetration testing methods, not to mention practical skills. It gives the feeling that education in the field of IS got stuck in the 80s of the last century, when the state was in a great need of cryptography specialists; a major bias in the field of fundamental knowledge; the lack of practice (again pen tests and all this here).

4. Reinforcement period - respecting a viable cybersecurity strategy at the workplace

One of the important directions in ensuring cybersecurity is the implementation of it at the workplace in each institution, public or private. You can use advanced software and hardware methods and means of ensuring cybersecurity, write the most correct and complete cybersecurity policies, but without the participation of all the employees of the company/institution, the effectiveness of the cybersecurity framework will be minimal. The human factor is the weakest link of any ISF.

Risks associated with human resources, the so-called personnel risks, are basic for all other types of risks that pose a threat to the stability of an economic entity. Moreover, in the area of risk formation again, the personnel decide everything. The entire enterprise management system directly depends on the personnel management system. The prevention and minimization of personnel risks is the main task in the human resource management process. It is necessary to take into account the fact that the conditions for the occurrence of such risks are present at each stage of the personnel management process.

The process of managing human resources in a company is continuous and is conditionally divided into several stages: the formation of personnel structure, the use of human resources and the release of personnel. Personnel and cybersecurity at all stages should be built at the forefront. The discrepancies between the qualitative and quantitative composition of the staff, the ineffectiveness of the selection procedures are only the main aspects that the organization may face [4].

The fact that the weakest-protected link in any process or system is the human being has been known since pre-computer times. Therefore, among other cyber-criminal situations prevail those in which, as a component of the information system, it is he (the man) who is being exposed. Cyber-criminals are actively using social engineering techniques when attacking him: according to Symantec Corporation, almost 70% of successful attacks are associated with it [5].

Practical implementation of all the provisions of the established cybersecurity policy will require from the company long-term practical efforts. One of the main and most difficult areas of employment is to work with the staff whose goals are the selection and preliminary inspection of

personnel recruited (for service); staff training; achievement of mutual understanding of managers and employees in matters of cybersecurity; psychological training in order to withstand the methods of the so-called “social engineering”.

In one of his books, Bruce Schneier, a well-known cybersecurity specialist, noted that the “mathematical system is impeccable in the general system of cybersecurity measures, computers are vulnerable, networks are generally lousy, and people are just abominable. I have studied many issues related to the security of computers and networks, and I can say that there is no solution to the problem of the human factor” [6].

This statement most clearly and vividly demonstrates the importance of targeted measures for the selection, placement and work with the personnel of the enterprise in order to prevent the creation of “bottlenecks” and so-called information systems and so on; the human factor has not become the most significant source of threats to cybersecurity. The main reason determining the importance of the human factor in the general system of information protection is that, with all the sophistication of modern automation tools, information systems continue to be man-machine complexes and their (systems) functioning depends largely on the work of individuals. It is for this reason that inadequate treatment of information system components by employees of an enterprise can cause serious damage to cybersecurity even if there are well-developed security policies and highly efficient software and hardware information protection.

In addition to careful selection, one of the important bases for working with personnel is its training in methods of ensuring cybersecurity and safe work with information systems. Training and the subsequent control of the received (available) knowledge can be both primary, and repeated. In general, the employee of an enterprise cannot be allowed to perform his or her duties and work with information systems until he/she has been trained in cybersecurity and will not: be familiarized in details with all the requirements and general applicable rules at the enterprise; be fully trained in the methods and techniques of ensuring cybersecurity necessary for the performance of his/her official duties; be acquainted with all possible measures of responsibility (disciplinary, administrative, criminal) that can be applied to him/her in case of violation of the requirements, as well as in the event of damage caused by his/her fault.

At the end of all preliminary work, the employee must give all the necessary commitments not to disclose confidential information, and testify in written form that he/she is fully familiar with the basic provisions of the security policy. In the course of work, an enterprise may also conduct periodic monitoring of knowledge and skills related to cybersecurity in order to attest to the competence of employees in this field. In addition, one of the training tools may be periodic staff familiarization with actual examples of recent incidents related to cybersecurity. Besides, additional training of enterprise personnel can be carried out in the following cases: the introduction of new automated information systems; changes in business processes of the enterprise; changes in security policy requirements (for example, due to changes in legal requirements).

The need for additional training in the implementation of new information systems and, in particular, integrated enterprise management systems, as a rule, may be due to the emergence of new software functionality and changes in information processing procedures. Also, the access to integrated information systems can potentially give access to previously inaccessible information and provide previously unavailable opportunities to influence various information flows. In this regard, it may be necessary for employees to make additional commitments to comply with cybersecurity measures. Similar organizational measures, to ensure the protection of information,

may be necessary when changing the enterprise business processes, when its structure changes, the distribution of functions between departments and employees' duties, and accordingly, changes are made to organizational charts, staffing tables and job descriptions of personnel. Changes in security policy requirements can be associated with the emergence of new threats, changes in legal requirements, expansion of markets, changes in the attitude of management and owners of the company to cybersecurity issues and other factors - all these clarifications and changes must also be fully and promptly communicated to staff.

In the process of learning, a clarification of rational reasons for which the company applies such a security policy may have some significance. This can serve both, better to understand and assimilate the positions of the security policy, as well as to relieve some of the psychological tensions that inevitably arise when taking restrictive measures and imposing additional duties, the necessity of which is not always obvious and understandable to ordinary employees and specialists.

A separate area of ordinary training and advanced training can be the development of company personnel skills to counter the methods of so-called social engineering (this approach is also sometimes called “sociotechnics”). The use of social engineering methods for illegal entry into information systems is associated with the so-called “human factor”, which is a combination of certain psychological inclinations and characteristics of thinking and behavior, which are peculiar to almost all the people. To the number of such propensities and features can be attributed: inability to adequately assess the danger in some situations; specific relation to rarely occurring events (dulled attention); excessive trust and reliance on automation; susceptibility to manipulation, based, for example, on the desire to help people (including strangers) or on excessive trust to people dressed in a special uniform, etc. [7].

To minimize the risks associated with human factors, it is necessary to organize a documented and approved work of the staff by the bank/company management towards awareness increasing and training in cybersecurity, including the development and implementation of plans, training programs and awareness-raising in the field of cybersecurity, as well as monitoring the results of the implementation of these plans.

Education of the personnel in the field of cybersecurity is necessary for the following purposes: developing and maintaining awareness among employees of the importance of safety in the use of information technologies, knowledge of the procedure for handling undesirable events and incidents; awareness of the employees of their role and place, as well as the duties and responsibility for ensuring the protection of information in the company; increasing the level of knowledge by employees of the basic rules of cybersecurity; communicating to employees the main positions, restrictions and requirements of existing documents (policies) in the field of cybersecurity; bringing to employees facts about which cybersecurity tools are used, as well as how to use these tools correctly and effectively.

The need to train and raise awareness of cybersecurity personnel is governed by the GD No. 201 Mandatory Cybersecurity Requirements of 03/28/2017, which requires public institutions to implement the Cybersecurity Management System. The head of the authority shall designate by administrative act the person (subdivision) responsible for the implementation of the cybersecurity management system in the institution and the responsible person shall be required to participate, at least once a year, in cybersecurity training courses and, respectively, to organize courses for the employees of the institution.

Cybersecurity education should include the following areas: raising awareness of workers in matters of cybersecurity (general course); safe work with personal data in the company; organization of business continuity and recovery after interruptions.

The main forms of education can be individual training (introductory, repeated and extraordinary briefings); special training with the involvement of external training centers; awareness raising: distance learning, social engineering methods (memos, posters, screen lockers, etc., reflecting all the requirements of the enterprises' regulatory documents on cybersecurity).

In accordance with the State Norms of Moldova, training and awareness plan requirements should be established for the frequency of training and awareness raising.

Unfortunately, a survey conducted last year on a sample of about 160 companies and institutions within a project to raise IT needs to increase cultural information and cybersecurity in Moldova shows that companies and institutions do not pay suffice important to cybersecurity (62% of respondents) and that they have a training program and awareness on cyber security (81% of respondents).It is also necessary to determine the list of documents that appear as evidence of the implementation of training and awareness-raising programs in the field of cybersecurity. Individual training (instruction) should be completed with an oral survey, and an assessment of the acquired skills of safe ways of work. The employee who conducted the briefing checks the knowledge.

With a distributed institution structure, it makes sense to impose responsibilities for training and awareness raising in the field of cybersecurity to a special employee appointed in each remote unit. As part of the self-assessment, the internal auditors of the institution should regularly monitor the level of awareness of employees of the audited units, the completeness and accuracy of the training documents, the timeliness of communicating new cybersecurity requirements.

The cybersecurity service should monitor the effectiveness of training by quantitative and qualitative analysis of the actions of employees, followed in response to certain events.

The training system under consideration is a scalable process aimed at constantly improving the level of knowledge, skills and qualifications in the field of cybersecurity of employees and integrates with existing business processes. As a result of the introduction of a training system and raising awareness in the field of cybersecurity in an institution, the number of incidents in this area related to human factors will be significantly reduced, as well as the misuse of resources.

Success and high security, including cybersecurity provides a continuous process of education and training of personnel in the field of cybersecurity. Training can be carried out in some areas and forms. Namely, the Complex Program: full-time courses; E-courses; Introductory briefings; posters; screensavers; animated and video clips; computer games; booklets, brochures, memos; souvenirs; efficiency mark, a comprehensive program to improve awareness of the company’s staff. What is good about an integrated approach in addressing issues of raising the awareness of company personnel in matters of cybersecurity? – It guarantees a high level of security of the company information resources; involves staff training cybersecurity on an ongoing basis; helps to manage the risk more effectively; has a positive effect on the company image; testifies to a high level of responsibility of the company management towards its employees; helps to prevent losses that are inevitable when staff of the company violates cybersecurity.

Introductory briefing for new employees. The familiarization with corporative security regulations for hiring is an important step towards conscious and strict adherence to corporative security rules by company staff. There can also be developed: an e-learning course on the rules of corporative security adopted by the organization; tests to check the level of knowledge of the company staff; educational flash and video clips on corporative security rules; illustrated memos on the main issues of the corporative security.

Posters. Thematic posters about corporative security issues are one of the most effective means of maintaining an atmosphere of corporative security and building a corporate culture of personnel on working safely with the company's information resources. Posters placed in all places accessible to the personnel of the company make it possible regularly to remind about the rules and requirements for ensuring corporative security adopted by the company.

Screensavers. The installation of corporative security screensavers is an effective way to remind the staff about the company's corporative security rules and regulations. It is recommended to update screensavers every 2 months to increase their effectiveness.

Animated and video clips – a bright and visual tool that allows in an attractive, unobtrusive way to convey to staff the rules and regulations for working with information resources of the company. Creating a corporative flash video on security issues: the flash movie script is developed in accordance with the organizational and administrative documentation of the institution in the field of corporative security and the corporate culture adopted by the company. The recommended duration of a flash movie is no longer than 1.5 minutes. The film assumes the use of announcer dubbing, including staged scenes with the involvement of actors, graphics. The shooting is carried out using professional equipment on the territory of the institution. The recommended duration of the video - 15 - 20 minutes.

Security Competitions (Cyber Drill, CTF**) or Computer games.** We offer a new look to the problem of compliance with the cybersecurity rules adopted by the company and to invite colleagues to participate. An entertaining cybersecurity quest is the best way to convey to employees the most important skills and knowledge.

In 2018, Information Technology and Cyber Security Service, in collaboration with European partners, Technical University of Moldova and some Moldovan private companies, managed to organize several Cyber Drill sessions for security officers from national companies and institutions. Also, the Technical University students organize annually CTF competitions and also participate in the international ones (Suceava, Bucharest, Volga, etc.)

Booklets, pamphlets, memos – are a convenient way to inform new employees about the company rules and regulations on corporative security. The memo written in simple, accessible language, the content of which reflects the main provisions of the safety regulations, is easy to use, has a bright, attractive aspect.

Evaluating the effectiveness of implementing an awareness-raising program is a very important phase of the awareness program. It is advisable to evaluate the effectiveness of the program after the staff has been trained and a number of measures have been implemented to maintain the corporative security atmosphere in the company. As part of the events, aimed at assessing the effectiveness of implementing an awareness-raising program. In this regard, you can send authorized provocative messages by corporative e-mail and SMS / MMS, which motivate users to

violate corporative rules and corporative security policies. The purpose of the work is to assess the implementation of basic corporative security rules by employees when using corporate e-mail and business cellular communications, in order to improve the program for raising awareness of corporative security issues.

In the framework of the work implementation to achieve the stated goals, the tasks of checking the elements of the program of raising awareness on the following issues are solved: password policies; compliance with license fairness; anti-virus attacks; complying with the rules of the IT services use in terms of the e-mail and the Internet utilization; abidance with cybersecurity rules when using service mobile devices and service cellular communication. Typical ways in which an enterprise can constantly remind its employees of the need to be careful are: placing and periodically changing (updating the design and content) reminders of the need to comply with the requirements of cybersecurity policies on items constantly in sight of employees during the working day: wall and desktop calendars, coffee mugs, covers of notebooks, desk exhibits, pens, pencils and other stationery; periodic emailing of relevant messages; use of screensavers containing relevant reminders; use of voice mail and speakerphone for periodic transmission of messages about the need to comply with cybersecurity rules, etc. [8].

5. Conclusions

We need to make security more of a realistic notion for the general public. A lot of users do not necessarily know where their data go. Rather than just corporate security awareness training, as professionals, we need to be bringing cybersecurity culture into the home as well.

Cybersecurity truly is a public safety issue. We have seen weaponized social media posts, IT devices turning into attack droids, and phones being hacked to see GPS locations. These issues are everyday occurrences. Therefore, we need to regulate the idea of security into our everyday culture, exactly the way we have normalized other safety issues. It could be illustrated by a simple example with cars. When it was found that the cars were unsafe, the seat belts were added.

For the Internet, we need a security-focused and educational mindset. This is especially the case in regards to innovations within technology. A scary awareness video is insufficient. In contrast, cybersecurity should be an ongoing education. The more we equip the public with this knowledge, the more efficient we will be in the future [9].

We would like to note that one of the main qualities that should be developed starting from school and cultivated at all subsequent stages is consciousness and awareness that a person is part of a whole class, group, working team, and that success, prosperity and security depends on his intellectual, spiritual and physical contribution. By instilling a sense of consciousness, the person will rejoice with all his might for the work that he is doing, and this is the best guarantee that cybersecurity and success in any business will be achieved.

6. References

[1] HAIBER, O. and MORRILL, S., Passport to the Future: A Secondary School Cyber Education Case Study, https://www.uscybersecurity.net/csmag/passport-to-the-future-a-secondary-school cyber-education-case-study/

[2] VIVEROS, M., Cyber Security Depends on Education, https://hbr.org/2013/06/cyber-security-depends-on-educ

[3] Геворг Маргаров, Воспитание защитников информации, https://www.osp.ru/os/2009/04/9298350

[4] Анастасия Богатырева, Кадровые риски, https://bisjob.ib-bank.ru/publikaciya/104

[5] Валерий Васильев, Дмитрий Сергеев, Человек — самое слабое звено в ИБ, http://www.infosecurity.ru/_gazeta/content/100305/art3.shtml

[6] Шнайер Б., Секреты и ложь. Безопасность данных в цифровом мире, СПб.: Питер, 2003.

[7] Александр Анисимов, Менеджмент в сфере информационной безопасности. Департамент информационной безопасности и работа с персоналом, http://www.intuit.ru/studies/courses/563/419/lecture/9580?page=2

[8] MITNICK, K. and SIMON, W., The Art of Deception: Controlling the Human Element of Security**,** Indianapolis (Wiley), 2002.

[9] TRICIA A. H., Cybersecurity Culture: The Root of the Problem, https://www.uscyber security.net/cybersecurity-culture/