PRO PUBLICO BONO – Public Administration, 2021/1, 128–147. • DOI: 10.32575/ppb.2021.1.8

Ion Bolun – Rodica Bulai – Dumitru Ciorbă

SUPPORT OF EDUCATION IN CYBERSECURITY

Ion Bolun, Professor, Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics, Departement of Software Engineering and Automatics, ion.bolun@isa.utm.md

Rodica Bulai, Lecturer, Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics, Departement of Software Engineering and Automatics, rodica.bulai@ati.utm.md

Dumitru Ciorbă, PhD, Associate Professor, Technical University of Moldova, Dean of the Faculty of Computers, Informatics and Microelectronics, dumitru.ciorba@fcim.utm.md

Cybersecurity depends heavily on education. The paper addresses the support of education as the smartest investment in cybersecurity. To define priorities, an early estimate of the state of cybersecurity in Moldova by an online survey has been completed. A wide range of aspects related to cybersecurity education are elucidated within three basic periods: initial (school), transit (university) and reinforcement (implementation and use at workplace). Referred to in these are: formation of an 'informational' culture, target professions, curricula content, competences, cooperation with companies, digital education, e-learning platforms, information services, risks associated with human resources, etc. Also, conceptual aspects regarding the creation of a cybersecurity polygon in support of training in the field are described: basic objectives, main functions, structural components, the technological platform and methodological issues of creating the system of cybersecurity models for application as needed.

Keywords:
cybersecurity, awareness, human errors, security incidents, survey, threats, vulnerabilities

1. INTRODUCTION

One of the most intriguing findings is that 95 per cent 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 in the field. Education in the field of cybersecurity is a necessary consideration for both individuals and families, as well as for businesses, governments and educational institutions.

We are facing an alarming shortfall of talent in cybersecurity. According to Cybersecurity Ventures, there will be 3.5 million unfilled cybersecurity jobs globally by 2021, up from one million positions in 2014[1] and of the candidates who apply, fewer than one in four are even qualified.[2] The U.S. Bureau of Labor Statistics predicts that cybersecurity jobs will grow by 31 per cent from 2019 to 2029, over seven times faster than the national average job growth of 4 per cent. Demand for information security analysts is expected to be very high, as these analysts will be needed to create innovative solutions to prevent hackers from stealing critical information or causing problems for computer networks.[3]

Given the rapid and continuous evolution of threats, it is critical that educational cybersecurity programs share best practices, curriculum and informatics support 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.

By 2020, more than half a million attacks have been estimated to occur in every minute.[4] Cybersecurity Ventures predicts cybercrime will cost the world in excess of $6 trillion in 2021[5] that is approximately 4 per cent of global GDP. At the same time, in the period 2005–2014, the share of group organised cyberattacks increased by four times, reaching approximately 80 per cent of the total.[6] Respectively, cyberattacks are becoming more sophisticated, and defending against them is increasingly difficult, requiring deep knowledge in the field; IT security is becoming an even higher priority, and companies are in dire need of security policies, security solutions and employee education workshops.

Even those employees who 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. During the

1 *The 2019/2020 Official Annual Cybersecurity Jobs Report* (Cybersecurity Ventures, 2020).
2 E Winick, 'A cyber-skills shortage means students are being recruited to fight off hackers', *MIT Technology Review,* 18 October 2018.
3 'Information Security Analysts', in Occupational Outlook Handbook, Bureau of Labor Statistics, U.S. Department of Labor.
4 V Voicu, 'Cybersecurity: Tendencies 2020', *Electronica Azi,* 06 April 2020.
5 *2019 Official Annual Cybercrime Report* (Cybersecurity Ventures, 2019).
6 L Ablon, M C Libicki and A Galay, *Markets for Cybercrime Tools and Stolen Information: Hackers' Bazaar* (Rand Corporation, 2014).

coronavirus pandemic, the cybersecurity of health services was tested, while the adoption of new work and distance learning, interpersonal communication, and teleconferencing regimes also changed cyberspace. In this period, cybercriminals have been expanding their capabilities, adapting quickly and targeting relevant victim groups more effectively.

The best defence is to provide comprehensive educational programs and informatics support for all. You do not 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.[7]

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), organisations 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 behaviour 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.[8]

The paper addresses issues related to basic periods of education in cybersecurity – initial (school), in transit (university) and reinforcement (at workplace) – and also related to adequate methodological and informatics support. First, an early estimate of the state of cybersecurity in the Republic of Moldova is presented to determine some priorities in the field.

2. STATE OF CYBERSECURITY IN THE REPUBLIC OF MOLDOVA

Out of the multitude of evaluations regarding informatisation in Moldova, few refer directly to cybersecurity.[9] Unlike the three indicators of 'Electronic Moldova'[10] and the four indicators

---

7 R Bulai, D Țurcanu and D Ciorbă, 'Cybersecurity in education', in *Proceedings of the CEE e|Dem and e|Gov Days 2019: Cyber Security and eGovernment* (Budapest, 2019).

8 M Viveros, 'Cyber Security Depends on Education', *Harvard Business Review,* 24 June 2013.

9 I Bolun, D Ciorbă, A Zgureanu, R Bulai, R Călin and C Bodoga, *State, Needs and Priorities of Information Security in the Republic of Moldova* (Chisinau: TUM, 2020).

10 'National Strategy for Building the Information Society – "Electronic Moldova"'. *Official Monitor* no 46–50, 25.03.2005.

of 'Digital Moldova 2020' strategies,[11] the 17 indicators of the 'Cyber Security Program' from 2016–2020[12] refer to the monitoring and evaluation of the policy documents in the field of information security implementation and not to assess the degree of cybersecurity achieved as a result of implementing the program actions. Also, the annual statistical reports 1-inf (Situation on informatisation and Internet connection) and 1-CE (Activity in the field of electronic communications) of the National Bureau of Statistics and the annual reports on the activity and evolution of ICT products and services market of the National Agency for Regulations in Electronic Communications and Information Technology do not contain indicators for assessing the degree of cybersecurity in the republic.

The only official sources of statistical data on cybercrime are the Register of Crimes, Criminal Cases, Criminals and Crime Materials, held by the Ministry of Internal Affairs and the Informatics system 'Criminal investigation: E-case', managed by the General Prosecutor's Office. However, the Republic of Moldova appears in some international evaluations in the domain, which show a slightly more advanced degree of cybersecurity in Moldova than the international average (Table 1).

Table 1 • *The Republic of Moldova in international cybersecurity rankings (Source: Compiled by the authors based on sources specified in the table.)*

No.	Index name	Total countries in the ranking	The Republic of Moldova's place in the ranking
1	Global Cybersecurity Index, GCIv3, y. 2018–2019[13]	175	53
2	Cyber Readiness Index, CRI 2.0, y. 2015[14]	125	N/A
3	National Cyber Security Index – NCSI 2018[15]	100	40
4	National Cyber Security Index – NCSI 2020[16]	152	52

The first, incipient estimate of the state of cybersecurity in Moldova was done in 2020 (May 25 – June 20) by an online survey.[17] Research was focused on enterprises/organisations/institutions (EOIs). Five categories of EOIs were defined according to the number of employees: very small – up to 10 employees, small – 11–50 employees, small-medium – 51–100 employees, medium – 101–500 employees and large – over 500 employees. In the survey, 24 indicators were used. They were determined based on

11 'National Strategy for the Development of the Information Society "Digital Moldova 2020"', *Official Monitor* no 252–257, 08.11.2013.

12 'National Cyber Security Program of the Republic of Moldova for the years 2016–2020', *Official Monitor* no 306–310, 13.11.2015.

13 *Global Cybersecurity Index 2018* (ITU, 2019).

14 Hathaway et al., *Cyber Readiness Index 2.0* (Potomac Institute for Policy Studies, 2015).

15 *National Cyber Security Index* (Tallin: eGovernance Academy, 2019).

16 Ibid.

17 Bolun et al., *State.*

respective international practice.[18] The survey results are described in the report of Bolun et al.[19]

The graph of the dependence of the percentage of EOIs (pEOIs) with high cybersecurity performance on indicators 1–23 are shown in Figure 1.

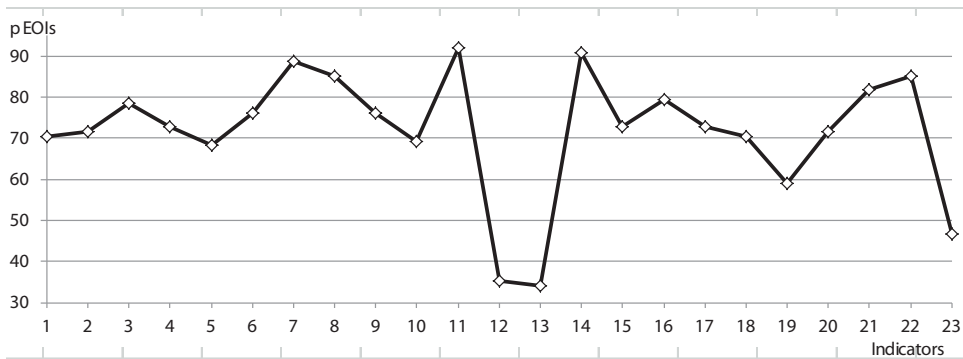

Figure 1 • *The %EOIs dependence on cybersecurity aspects 1–23 (Source: Compiled by authors.)*

Figure 1 shows that EOIs percentage in cybersecurity varies from 34.1 per cent to 92.0 per cent. Only at 34.1 per cent of EOIs is ensured, high cybersecurity performance in terms of Intrusion Prevention Systems/Wireless Intrusion Prevention Systems (IPS/WIPS) use at all perimeter nodes of the EOI informatics network (indicator 13) and, likewise, the use of Intrusion Detection Systems/Wireless Intrusion Detection Systems (IDS/WIDS) at all perimeter nodes of the EOI informatics network (indicator 12 – 35.2 per cent). These two indicators are critical (the least EOIs have high cybersecurity performance). Also, the cybersecurity audit of informatics space is performed only at about 46.6 per cent of the EOIs. A low degree of cybersecurity is also in terms of testing external and internal penetration to identify vulnerabilities and attack vectors on EOI informatics space (indicator 19 – 59.1 per cent), the use, in sensitive cases, of secure dedicated computers (indicator 5 – 68.2 per cent) and performing the iSecurity Audit of new informatics applications/systems before implementation (indicator 10 – 69.3 per cent). On the other hand, the best situation is with the automatic creation of backups of sensitive information on secure servers (aspect 11 – 92.0 per cent). A relatively high degree of cybersecurity is also important in terms of regulating access to resources (aspect 14 – 90.9 per cent), the use of VPN (aspect 7 – 88.6 per cent), the use of firewalls (aspect 8 – 85.2 per cent) and informing employees about the implications of informatics security, including possible malicious software (aspect 22 – 85.2 per cent). Overall, the average degree of EOIs

[18] *ETSI GS ISI 001-1 V1.1.1 (2013-04) Information Security Indicators* (ETSI, 2013); *CIS Security Metrics* (Center for Internet Security, 2010); *CIS Controls v. 7.1 Measures and Metrics* (Center for Internet Security, 2019).

[19] Bolun et al., *State.*

cybersecurity (based on the 23 indicators) is about 71.7 per cent; that is, in 71.7 per cent of cases, regarding the 23 indicators, high cybersecurity performance is ensured.

For a more detailed comparison, Figure 2 shows the graph of the dependence on indicators 1–23 of pEOIs by categories according to the number of employees. It clearly indicates the big difference between the cybersecurity state of large EOIs (over 500 employees) and of the small ones (up to 10 employees inclusive) for each of the 23 indicators.

It should be noted that in case of EOIs with up to 10 employees, IPS/WIPS at all perimeter nodes of the corporate network are not used (indicator 13) nor is the cybersecurity audit of the informatics space performed (indicator 23) in any EOI. Among these, the number of EOIs using IDS/WIDS at all perimeter nodes of the corporate network (indicator 12), using dedicated VLANs (indicator 6) and testing external and internal penetration to identify vulnerabilities and attack vectors (indicator 19) is also reduced. Moreover, few such EOIs have implemented an internal iSecurity policy (indicator 1) and internal iSecurity regulations (indicator 2) and have a recovery plan in case of iSecurity incidents (indicator 3).

Significantly better than at EOIs with up to 10 employees is the state of iSecurity at EOIs with 11 to 50 employees. However, only 20 per cent of them use IDS/WIDS (indicator 12) and IPS/WIPS (indicator 13) at all perimeter nodes of the corporate network and only 52.6 per cent of them have implemented an internal iSecurity policy (indicator 1) and tests external and internal penetration to identify vulnerabilities and attack vectors (indicator 19).

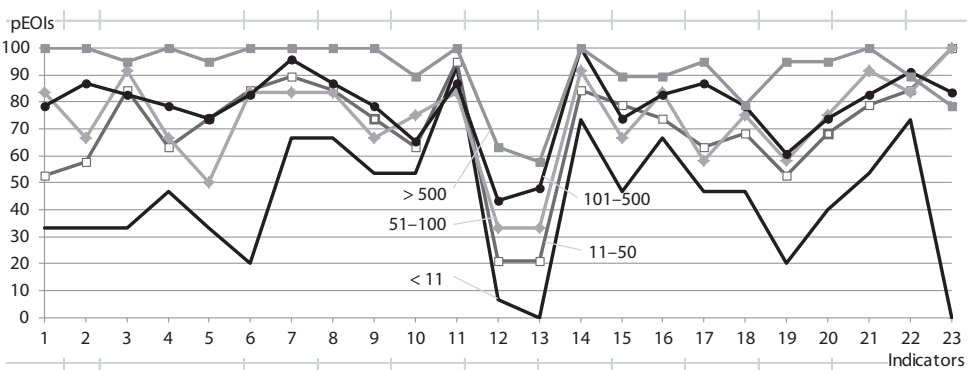

Figure 2 • *Dependence of pEOIs, by categories according to the number of employees, on indicators 1–23 (Source: Compiled by authors.)*

On average, the percentage of EOIs with high cybersecurity performance for EOIs with over 500 employees (91.7 per cent) is about twice as high as that for EOIs with up to 10 employees (43.8 per cent).

Thus, even according to this narrow set of 24 indicators (for example, the ETSI set contains 97 indicators,[20] and the CIS Controls one – 171 indicators[21]), it can be concluded that the state of Moldovan EOIs cybersecurity is relatively low, which confirms the need for additional measures in the field. It is also important, in the respective training courses, to draw special attention to aspects with a relatively low cybersecurity performance.

3. 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 with education in 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 – familiarisation – 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 familiarisation 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; discipline training while working on the network.

The trainees should know: the list of the Internet information services; the rules of 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 a web-browser; use information resources; search for information on the Internet.

A good start for the Republic of Moldova is that on 14 June 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 were collected for the procurement of digital tablets and laptops in support of teachers across the country. The 'Digital Education' module is compulsory for 1st

[20] *ETSI GS ISI 001-1 V1.1.1 (2013-04) Information.*
[21] *CIS Controls v. 7.1 Measures.*

grade pupils and optional for those of 2–4 grades. In this respect, it is important that Digital Education also develops a cybersecurity culture; cybersecurity education modules must be included in every curriculum of Informatics for all the grades from the 1st to the 12th.

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 Police General Inspectorate has been involved in a number of projects such as, *Together we make the Internet better!* and, *An informed child – A protected child,* for the protection of children's rights and needs in the Republic of Moldova. We realise that we all have a common responsibility to make cyberspace safer for everyone, especially for children, namely through information, education and awareness.

4. THE TRANSIT PERIOD – THE UNIVERSITY – THE STUDY AND DEVELOPMENT OF THE PRINCIPLES AND STANDARDS TO ENSURE AND HAVE RESPECT FOR CYBERSECURITY

Methods and cybersecurity technologies – is the youngest area of IT in our country. The other areas – software, hardware, service – on 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 analysed: legislatively approved qualification requirements of the Republic of Moldova state institutions; requirements for civil servants working in the field of cybersecurity; recently established professional standards in the field of IT and IS; various international standards for the protection of information, from which one can learn much valuable information about what different levels specialists should be able to do; regulatory documents existing at enterprises describing the functional responsibilities of such specialists, and so on.

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.

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 and 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 organisational and legal aspects of ensuring cybersecurity should be included in the limited scope of the curriculum.

The complex of technical disciplines for students of cybersecurity is also optimised – they study various aspects of cybersecurity in the physical environment and the features of the organisation 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 organisational issues of cybersecurity, which is also dedicated to a separate discipline.

Between 10 July and 31 October 2017, a survey was conducted to identify the target professions and training needs in the field of IT security in Moldova.[22] The questionnaire, containing 23 questions, was completed by 199 companies – IT companies, the provider companies of electronic communication services and banks, which demonstrates an increased interest from companies in the field of cybersecurity. Almost 69 per cent of professionals in the field specified that they need additional training in computer security. Based on this survey, in 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 license and master programs in Cybersecurity, an analysis of European curriculum documents has been carried out as well: 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, and so on.

At these four universities, the targeted training of specialists for the Central Bank, the Ministry of Internal Affairs, and other state institutions of the Republic of Moldova is conducted. This approach has a number of advantages. The organisation, 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 a professional and moral point of view, which is important for working in the field of cybersecurity. Likewise, specialists of enterprises with whom the faculty cooperates, actively participate in educational process, and this involvement of practitioners in teaching allows maintaining the relevance of the courses.

Currently there is a technical-scientific centre at the Technical University of Moldova. In fact, it has also become the centre of crystallisation 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 centre is gradually turning into a mini technology 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.

[22] Bolun et al., *State*.

Such a synthesis of business and education allows the university independently to earn money to improve its educational process and to attract highly qualified specialists to teach and improve the professional level of its employees.[23]

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 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.

Therefore, we believe that the effect brings 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 organised. 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 the 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.[24] 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. At the beginning, 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 society, the problems of information protection become more substantial, which determine the emergence of specialties related

[23] Bulai et al., 'Cybersecurity in education'.

[24] Г Маргаров, 'Воспитание защитников информации' [Educating defenders of information], Открытые системы 28, no 4 (2009).

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 a 'third literacy' along with 'second literacy' – computer skills and information technology.

5. 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. One 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 minimisation 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.[25]

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 and the ineffectiveness of the selection procedures are only the main aspects that the organisation may face.[26]

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 prevailing cybercriminal situations, those in which, as a component of the information system, it is the person that is being exposed. Cybercriminals are actively using social engineering techniques when attacking them: according to the Symantec Corporation, almost 70 per cent of successful attacks are associated with it.[27]

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

[25] Bulai et al., 'Cybersecurity in education'.
[26] A Bogatiriova, 'Personnel risks'.
[27] Васильев, В and Д Сергеев, 'Человек — самое слабое звено в ИБ' [Man is the weakest link in information security].

inspection of personnel recruited (for service); staff training; achievement of the mutual understanding of managers and employees in matters of cybersecurity; psychological training in order to withstand the methods of 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'.[28]

This statement most clearly and vividly demonstrates the importance of targeted measures for the selection, placement and work with the personnel of an 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 familiarised in details with all the requirements and generally 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 familiarisation 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,

[28] Б Шнайер, *Секреты и ложь. Безопасность данных в цифровом мире* (СПб.: Питер, 2003).

due to 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 the 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 social engineering. 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 behaviour, which are peculiar to almost all 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 of people dressed in a special uniform, and so on.[29]

To minimise the risks associated with human factors, it is necessary to organise a documented and approved work of the staff by the company management towards increasing awareness 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 an administrative act the person responsible for the implementation

[29] А Анисимов, *Менеджмент в сфере информационной безопасности* (Департамент информационной безопасности и работа с персоналом) [Information Security Management. Information Security Department and Human Resources].

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 organise 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; organisation 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 centres; awareness raising: distance learning, social engineering methods (memos, posters, screen lockers, and so on, 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 in 2018 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 sufficient importance to cybersecurity (62 per cent of respondents) and that they do not have a training and awareness program on cybersecurity (81 per cent 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 the safe ways of work. The employee who conducted the briefing should check 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 and 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 integrated 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 an improvement in the misuse of resources will become apparent.

Success and high security, including cybersecurity, provide 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. *Security Competitions (Cyber Drill, CTF) or Computer games,* 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 the most important skills and knowledge to employees.

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

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 a corporate security atmosphere in the company. Part of the events should be aimed at assessing the effectiveness of implementing an awareness-raising program. In this regard, you can send authorised, provocative messages by corporate e-mail and SMS/MMS, which motivate users to violate corporate rules and corporate security policies. The purpose of the work is to assess the implementation of basic corporate security rules by employees when using corporate e-mail and business cellular communications, in order to improve the program for raising awareness of corporate 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 IT services use in terms of e-mail and Internet utilisation; abidance with cybersecurity rules when using service mobile devices and cellular service 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, and so on.[30]

[30] K Mitnick and W Simon, *The Art of Deception: Controlling the Human Element of Security* (Indianapolis: Wiley, 2002).

6. A CYBERSECURITY POLYGON IN SUPPORT OF EDUCATION

In support of education, experimentation, research, adaptation and development (EERAD-ment) in cybersecurity in the Republic of Moldova, the PINFOSEC polygon is being implemented.[31] The polygon will create conditions, provide necessary infrastructure and tools for EERAD-ment, based on which practical recommendations will be elaborated and differentiated cybersecurity solutions will be proposed, taking into account the particularities of the republic. The basic objectives of PINFOSEC polygon consist in:

1. Creation of an extensive technological platform for the EERAD-ment of cybersecurity solutions (SECIM)
2. Development of SECIM modules for the EERAD-ment of cybersecurity solutions
3. Development of a system of cybersecurity models (SIMOSI) for application as needed
4. Implementation of SECIM modules within the SIMOSI system, research through simulation of their cybersecurity features and further the afferent, depending on the case, cybersecurity solutions development to strengthen performance
5. Integration with the INFOSEC website for differentiated information of public administration institutions, economic agents, organisations and population regarding the dangers, vulnerabilities, incidents, means and necessary actions of cybersecurity and of other important aspects in the field, thus forming the PINFOSEC informatics space (iSpace)

PINFOSEC iSpace will be created as a secure virtual computer network (RINFOSEC) within the Technical University of Moldova (TUM) Informatics Network. Within RINFOSEC, equipment can be used only within the PINFOSEC iSpace. PINFOSEC means will be used to create, configure and emulate various informatics infrastructures and cyber incident situations, intended for the EERAD-ment of cybersecurity means in accordance with objectives defined above. Therefore, RINFOSEC will include such informatics means as: network stations, routers, switches, wireless access points, data transfer channels, transmission media, including wireless ones, software tools, computer applications, specialised software, various information resources, and so on. The basic technological solution of resource cooperation for exploring the PINFOSEC iSpace will be a client–server one.

As mentioned above, the SECIM platform will form the technological support of cybersecurity means that will be EERAD-ed within the PINFOSEC polygon. One of them is the *EduSec* educational platform – a special environment for training, awareness programs, training of hacking skills, and so on.

SECIM modules will be adaptations/developments of some means of cybersecurity. They will be developed using as a starting point, for example, the CIS Controls set of actions/sub-controls[32] or similarly, including those aimed at meeting the performance requirements, as

[31] I Bolun, D Ciorbă, A Zgureanu, R Bulai, R Călin and C Bodoga, *Report "PINFOSEC polygon concept"* (Chisinau: TUM, 2020).

[32] *CIS Controls v. 7.1 Measures.*

measured by the ETSI Information Security Indicators.[33] Based on SIMOSI cybersecurity models, concrete differentiated cybersecurity solutions will be generated, adapted to needs of various categories of entities in Moldova, considerably facilitating the respective activities and, at the same time, strengthening the expected effects. The SECIM platform extensibility will allow the resultant continuation of the EERAD of cybersecurity solutions in rhythm with the advancement of theoretical results and of practical means in the field.

7. CONCLUSIONS

Cybersecurity depends a lot on education. We need to make security more of a realistic notion for the general public. A lot of users do not necessarily know the destination of their data. Rather than just corporate security awareness training, as professionals, we need to be bringing cybersecurity culture into people's homes, as well.

Cybersecurity truly is a public safety issue. We have seen weaponised 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 normalised other safety issues. It could be illustrated by a simple example with cars. When it was found that the cars were unsafe, 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.[34]

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 a part of a whole class, group, working team, and that success, prosperity and security depends on each individual's intellectual, spiritual and physical contribution. By instilling a sense of consciousness, the person will rejoice for the work that is being done, and this is the best guarantee that cybersecurity and success in any business will be achieved.

In order to strengthen the training activities, the critical aspects regarding the EOIs cybersecurity are identified and some aspects of the creation of a cybersecurity polygon are approached. It is estimated that PINFOSEC polygon will significantly contribute to ensuring the necessary conditions for improving the education in cybersecurity.

[33] *ETSI GS ISI 001-1 V1.1.1 (2013-04) Information.*

[34] T A Howard, 'Cybersecurity Culture: The Root of the Problem', *United States Cybersecurity Magazine.*

REFERENCES

1. *2019 Official Annual Cybercrime Report.* Cybersecurity Ventures, 2019. Online: www.herjavecgroup.com/wp-content/uploads/2018/12/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf
2. *The 2019/2020 Official Annual Cybersecurity Jobs Report.* Cybersecurity Ventures, 2020. Online: www.herjavecgroup.com/2019-cybersecurity-jobs-report-cybersecurity-ventures
3. Ablon, L, M C Libicki and A Galay, *Markets for Cybercrime Tools and Stolen Information: Hackers' Bazaar.* Rand Corporation, 2014. Online: https://doi.org/10.7249/RR610
4. Анисимов, А, *Менеджмент в сфере информационной безопасности.* Департамент информационной безопасности и работа с персоналом [Information Security Management. Information Security Department and Human Resources]. Online: www.intuit.ru/studies/courses/563/419/lecture/ 9580?page=2
5. Bogatiriova, A, 'Personnel risks'. Online: https://bisjob.ib-bank.ru/publikaciya/104
6. Bulai, R, D Țurcanu and D Ciorbă, 'Cybersecurity in education' in *Proceedings of the CEE e|Dem and e|Gov Days 2019: Cyber Security and eGovernment.* Budapest, 2019. Online: https://doi.org/10.24989/ocg.v335.2
7. Bolun, I, D Ciorbă, A Zgureanu, R Bulai, R Călin and C Bodoga, *Raportul "Conceptul poligonului PINFOSEC"* [Report "PINFOSEC polygon concept"]. Chisinau: TUM, 2020.
8. Bolun, I, D Ciorbă, A Zgureanu, R Bulai, R Călin and C Bodoga, *Starea, necesitățile și prioritățile securității informatice în Republica Moldova* [State, Needs and Priorities of Information Security in the Republic of Moldova]. Chisinau: TUM, 2020.
9. *CIS Security Metrics.* Center for Internet Security, 2010. Online: www.itsecure.hu/library/image/CIS_Security_Metrics-Quick_Start_Guide_v1.0.0.pdf
10. *CIS Controls v. 7.1 Measures and Metrics.* Center for Internet Security, 2019. Online: www.cisecurity.org/white-papers/cis-controls-v7-measures-metrics
11. *ETSI GS ISI 001-1 V1.1.1 (2013-04) Information Security Indicators.* ETSI, 2013. Online: www.etsi.org/deliver/etsi_gs/ISI/001_099/00101/01.01.01_60/gs_isi00101v010101p.pdf
12. *Global Cybersecurity Index 2018.* ITU, 2019. Online: www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
13. Hathaway, M, Ch Demchak, J Kerben, J McArdle and F Spidalieri, *Cyber Readiness Index 2.0.* Potomac Institute for Policy Studies, 2015. Online: www.potomacinstitute.org/images/CRIndex2.0.pdf
14. Howard, T A, 'Cybersecurity Culture: The Root of the Problem'. *United States Cybersecurity Magazine.* Online. www.uscybersecurity.net/cybersecurity-culture
15. 'Information Security Analysts', in Occupational Outlook Handbook, Bureau of Labor Statistics, U.S. Department of Labor. Online: www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

16. Маргаров, Г , 'Воспитание защитников информации' [Educating defenders of information]. Открытые системы 28, no 4 (2009). Online: www.osp.ru/os/2009/04/9298350
17. Mitnick, K and W Simon, *The Art of Deception: Controlling the Human Element of Security*. Indianapolis: Wiley, 2002.
18. *National Cyber Security Index*. Tallin: eGovernance Academy, 2019. Online: https://ncsi.ega.ee/methodology
19. 'Programul național de securitate cibernetică a Republicii Moldova pentru anii 2016–2020 [National Cyber Security Program of the Republic of Moldova for the years 2016–2020]'. *Monitorul Oficial* no 306–310, 13.11.2015.
20. 'Strategia Națională pentru Edificarea societății informaționale – "Moldova electronică" [National Strategy for Building the Information Society – "Electronic Moldova"]'. *Monitorul Oficial* no 46–50, 25.03.2005.
21. 'Strategia Națională de dezvoltare a societății informaționale „Moldova digitală 2020" [National Strategy for the Development of the Information Society "Digital Moldova 2020"]'. *Monitorul Oficial* no 252–257, 08.11.2013.
22. Шнайер, Б, *Секреты и ложь. Безопасность данных в цифровом мире* [Secrets and lies. Data security in the digital world]. СПб.: Питер, 2003.
23. Васильев, В and Д Сергеев, 'Человек — самое слабое звено в ИБ' [Man is the weakest link in information security]. Online: www.infosecurity.ru/_gazeta/content/100305/art3.shtml
24. Viveros, M, 'Cyber Security Depends on Education'. *Harvard Business Review,* 24 June 2013. Online: https://hbr.org/2013/06/cyber-security-depends-on-educ
25. Voicu, V, 'Cybersecurity: Tendințe 2020 [Cybersecurity: Tendencies 2020]'. *Electronica Azi,* 06 April 2020. Online: www.electronica-azi.ro/2020/04/06/cybersecurity-tendinte-2020
26. Winick, E, 'A cyber-skills shortage means students are being recruited to fight off hackers'. *MIT Technology Review,* 18 October 2018. Online: www.technologyreview.com/2018/10/18/ 139708/a-cyber-skills-shortage-means-students-are-being-recruited-to-fight-off-hackers

Ion Bolun is a Professor at the Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics, Department of Software Engineering and Automatics. His field of research is performance analysis, synthesis and configuration of computer networks and systems and, tangentially, securing electronic transactions and optimisation in decision-making systems. Some of the latest research refer to such aspects of proportional apportionments among beneficiaries of discrete entities as: optimisation criteria to use, the 'population paradox' and the favouring and the full favouring of large or of small beneficiaries by well-known and widely applied apportionment methods.

Rodica Bulai is a Lecturer at the Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics, Department of Software Engineering and Automatics. In 2011, she contributed to the opening of a new study program Information Security, cycle I, Bachelor, and in 2018 cycle II, Master, which she coordinates so far successfully. Her field of research is the improving of management in Information Security, efficient management of vulnerabilities, optimisation of risk analysis methodologies; solutions, tools and controls for prevention and protection against threats, attacks, fraud in the digital environment. An important field is also the education in the field of information security, training and awareness platforms, programs and teaching tools, analysis of the performance of cybersecurity training methods.

Dumitru Ciorbă is an Associate Professor at the Technical University of Moldova, Faculty of Computers, Informatics and Microelectronics. The faculty, where Mr Dumitru Ciorbă is the Dean, is a centre with a balance and synergy between education and research – there are four departments and several research centres. He has teaching experience in various fields of IT, but his scientific research is mainly focused on object-oriented analysis and design, distributed and concurrent programming, and software architecting. Also, computer-based learning methods define another area of his interest, engineering education, promoting the use of modern learning management systems in the faculty's education process.