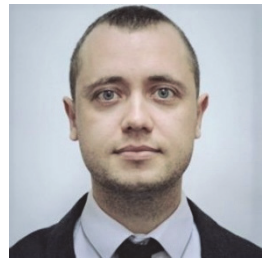

Sustainable cybersecurity training for modern society

Tudor Bragaru[1], Valentin Briceag[2]
Moldova State University, Chisinau, A. Mateevici, 60, MD-2009, Republic of Moldova
[1]tbragaru@usm.md, [2]valentinbriceag@gmail.com

Abstract: The ongoing training of the whole cybersecurity (CS) culture of the whole society level starts with the classification of users, continues with the definition of the needs/areas of CS, the identification of the appropriate forms and tools of training. And maintaining a strong CS culture is possible only through a continuous process of updating, measuring, assessing and repeating training. The paper aims to promote a conscious and responsible attitude towards continuing and sustainable Cybersecurity education by training target groups, such as broad masses of end-users outside corporations, corporate users by categories, including CS professionals by fields and types of industries.

Keywords: Cybersecurity, Awareness, Training, Education, Professional Development, Certification.

1 Actuality of Cybersecurity

Today we live in a dynamic and interconnected global information environment, based on modern information and communication technologies *(I&CT, shortly IT)*: Personal computers, Tablets, Smartphones, iPhones, IoT/IoB *(Internet of Things/Internet of Bussines),* Smart home, Internet, Web, Social networks, Cloud computing, electronic payments, Online education, Distance learning/working, etc. If 20 years ago online presence was more of a style, today, online presence has become a vital necessity: presence on various social networks, official sites, business, education, games, entertainment, various insecure objects connected to the Internet; the massive online transition, much accelerated in the last 2 years by COVID 19, Internet and Web, electronic transactions in cyberspace, regardless of the business size. People, organizations, businesses want easy access to everything from products to services and transactions, including access to information, often just a "click away". Systems, people, and related devices exchange huge amounts of data, documents, photos, audio, video, and more.

Simultaneously with the expansion and penetration of IT in all spheres of human life, ranging from a simple smartphone to complex information systems that manage critical infrastructure, cyber threats are constantly evolving, affecting everyone. Also, cyber risks give rise to geopolitical, economic, national security, reputation and privacy issues. Threats are becoming more sophisticated and growing exponentially. Despite an excessive tendency on focusing CS only on the technical-technological aspect, it is based on three pillars: "people, processes and technology", the weakest link being the human component. Only technical measures for more than

twenty years have ceased to be sufficient for safe operation in cyberspace. Any connected entity and/or network user may face cyber-attacks: spear-phishing, spam, scam, ransomware, malware, Denial-of-service attacks *(DoS)*, *DDoS* – Distributed DoS, *PDoS* – a Permanent Denial of Service and *TDoS* – a Telephony Denial of Service, three types of DoS attacks, that can compromise telephone system, computer hardware, theft of information or identity, etc., used by attackers for scam, money laundering, industrial espionage, etc. Currently attackers avoid "classic" attempts such as intrusion, DDoS, etc. Instead, they prefer attacks on people: either employees or customers, or third parties, often combining phishing and social engineering.

The aftermath of today's cyberattacks can be:

- Damaging the reputation of a company/person by changing a brand on the Internet, distorting a website, etc.;
- Withdrawal of funds, such as embezzlement of bank websites and ransomware;
- Espionage to steal company or government secrets;
- Total sabotage IT/Information Systems *(IS),* infrastructure blockage.

Faced with sophisticated attacks, politicians are beginning to realize that the response to the CS must also be state-led. Thus, for more than twenty years, CS cybersecurity has become an issue, which all leaders and those responsible should take into account on a permanent basis to ensure a secure and stable cyberspace as the basis for the functioning of modern society.

Private, state-owned enterprises, government agencies, both large and medium and small - are all vulnerable to cyber intrusions. Cyber-risks and attacks target all interconnected individuals/private and legal entities, national economies, critical national and corporate infrastructures and all valuable information assets.

All entities that process sensitive data must implement advanced cybersecurity systems. At the same time, by virtue of global connectivity, CS also refers to all interconnected users, not just the people responsible for the organization and management of CS. According to [1] at the beginning of 2021, there were almost 4.88 billion Internet users or over 67.1% of the world's population, with over 27 billion networked devices spending an average of about 3.5 hours a day on the Internet. On social networks alone, about 4.55 billion Internet users or 57.6% of the world's population are present on a daily basis, their number being constantly increasing by 409 million annually.

2 Awareness, training, education is the key of cybersecurity

Several researches in the field of CS focus on the "human factor", in the context in which people are considered the weakest link, one of the main weaknesses exploited by cyber attackers. Researchers associate 70% to 95% of CS incidents undergone by states, organizations, individuals due to human error.

According to a study by IBM, Cybint and others, "Human error is the main cause of 95% of Cybersecurity breaches. In other words, if human error was somehow eliminated entirely, 19 out of 20 cyber breaches may not have taken place at all" [2]. Human error occurs either because of a lack of qualification, or because users fail to adopt safe CS practices, or because they are unaware of the risks of CS, or because they do not understand the implications of violating security procedures, or because they do not understand how which they must act on, etc. Such errors include poor passwords, disclosure of sensitive information on social networks, neglect or carelessness regarding certain emails and phone calls, misuse of corporate IT resources, and so on. According to the same study and NIST [3], the key to reducing losses due to the human factor is the proper training of users of any level, each according to its role and needs *(Fig. 1)*.

NIST intends to upgrade SP 800-50 published in 2003 [3] to include privacy and add potential by consolidating with SP 800-16 (Information Technology Security Training Requirements: a Role and Performance Based Model), originally launched in 1998 and revised in 2014. The new proposed title for up-to-date version SP 800-50 Revision 1 is "Building a Cybersecurity and Privacy Awareness and Training Program".

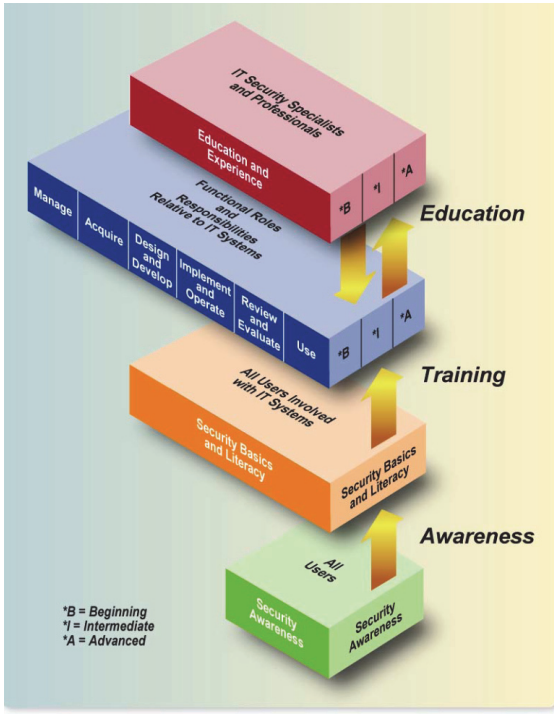

Figure 1. The IT Security learning continuum [3]

Online security has become one of the most pressing issues in the modern world, and cybersecurity awareness has become a vital necessity for everyone. Ongoing and sustainable training for the protection of IT users in the dynamic cyberspace is becoming increasingly important against the background of the increasing number of significant incidents of CS and the growing dependence on IT. This fact is recognized globally by adopting the numerous standards and recommendations of good practices, developed by ISO, IEC, ITU, NIST, ISACA (Information Systems Audit and Control Association, founded in 1967 in USA, *www.isaca.org*), ENISA (European Network and Information Security Agency, founded in 2004, *https://www.enisa.europa.eu*) etc. to steer institutions and organizations towards organizational e-transformation capable of responding to cyber-attacks, fact confirmed by the ever-increasing demand for Cybersecurity culture training programs.

Correct use of terminology

A lasting formation of the CS culture starts from the clarification of the terminology. The fields of security are booming, the terminology has changed significantly over the years, with many different meanings and connotations [4]. There are currently dozens of related terms in the world related to computer/digital security, security of IT, IS, IoT/IoB, Cloud Computing Security, computers, information, corporate network, critical infrastructure security, etc. On the other hand, there is a lack of a clear relationship and delimitation between the different concepts of security.

Indeed, the great diversity of terms can overwhelm anyone. People often confuse the concepts of computer security – information security – Cybersecurity, etc., do not have a clear vision of the boundaries and relationships between them. In fact, although these concepts are closely related, they differ a lot in terms of tasks, areas of coverage, functions, etc. Briefly, information security includes all other types of security as interdependent architectural components (Fig.2).

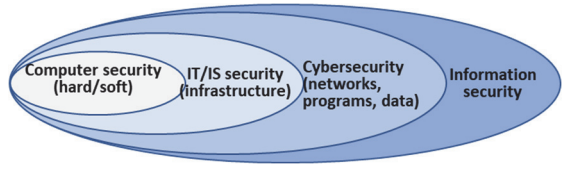

Figure 2. Correlation of security components

Information security, generally, refers to the **security of any information assets**, including paper documents, oral, voice, verbal, visual, digital information, mobile, media, etc. At the highest state level, this includes various other issues, such as media security, propaganda, censorship, social manipulation, cyber espionage, etc. Formally, information security is defined in the standard ISO/IEC 27000 [5]: Information security involves ensuring the protection of the fundamental characteristics of information: **Confidentiality**, **Integrity** and **Availability**, in the literature referred to as the **CIA triad**. However, in addition to preserving the CIA triad, various regulatory bodies e.g. *ISO, IEC, ITU, NIST, ISACA, ENISA,* etc.

require the assurance of other additional CIA-based attributes, such as the **right to possess information**, **the authenticity** of information *(ensuring that a message, transaction, or other exchange of information comes from the source it is claimed to be),* non-repudiation *(inability to deny the issuance of information and easy verification of the issuer),* reliability *(degree of trust)*"[5-8] and others. In turn, the field of information security includes Cybersecurity, IT/IS security, etc. up to the lowest level of computer security, media, codes used, etc.

Security of computers/operating terminals managed by end users, often connected to the corporate network via the Internet, in fact it refers to any smart device, with working memory, processor, operating system, including mobile phone and is the main target of attack hackers, viruses, spam, scams, phishing, social engineering, and many other threats, which come mainly from the Internet. Usually, at this level, protection is implemented by reducing certain organizational or technical-technological security vulnerabilities in computing and telecommunications systems, including devices for storing, processing and transmitting information mainly through configurations.

IT/IS security is self-contained and is based on computer security, but is not limited to purely technical-technological security. In addition, it includes many other related tasks, such as compliance with security requirements, information risk management, IT/IS security performance management, business continuity, etc. These and other similar tasks of IT/IS security require the skills of economists, managers, lawyers, financiers, psychologists, teachers, etc. Thus, IT/IS security goes from the purely technical-technological level to the competent management level of IT/IS and, sooner or later, it comes down to information security in understanding the standard ISO/IEC 27001 [7].

Cybersecurity [8] is the most ambiguous term, often being assigned to one or more of its wide ranges of related areas, e.g., physical and logical security of software and technical infrastructures, computer security, network security, technology security, IT/IS security, human component security, etc. Some people think that cybersecurity is the same as IT/IS security or information security or computer security. Others consider CS to be a new level of IT/IS security in the Internet environment.

Briefly, Cybersecurity means information security in control systems and/or complex information systems and, in any case, is reduced to information security management within the meaning of ISO/IEC 27001. Both concepts refer to CIA preservation, but also to protect other secondary properties based on the CIA triad. However, while *CS refers to a threat which may exist or not in cyberspace*, e.g., protection of social media accounts and other active in digital format in cyberspace, *information security refers to both digital and non-digital information in physical format*, e.g., paper., oral, vocal information, etc. CS is the largest and most important part of information security, covering about 95% [4].

In essence, SC covers a set of methods, technologies, and processes designed to protect the integrity of networks, programs, and data from digital attacks. In practice, CS refers to the protection of the CIA triad only for the valuable information and data of the company, circulated in cyberspace. From an architectural point of view CS consists of a very complex and varied set of problems with the operation of IT/IS software in cyberspace, data protection, systems and related infrastructures, in order to keep them safe anytime in order to ensure business continuity, either before, during, or after an unwanted attack or incident. Issues can range from simple, narrow, such as enforcing configuration standards, investigating incidents to the most extensive and complex, such as performance analysis and continuous improvement of information security.

Other variations in the interpretation of the concept of "Cybersecurity" according to ISO/IEC 27032 [8] emphasize the human component: protection

against political, physical, spiritual, emotional, educational, professional, psychological and other influences, as well as the consequences of urgency, errors, accidents, damages, injuries and other events that take place in cyberspace, which are considered undesirable. The set of conditions under which all objects in cyberspace are protected from the maximum possible number of known threats, as well as from impacts with undesirable consequences.

From the paper, the terms CS and Information Security can be considered synonymous because their functions are largely intertwined, but their fine line of demarcation must also be taken into account.

CS awareness for the widest masses of users

Promoting the culture of information security to enable users of all levels to comply with **information security policies, rules and procedures** is largely associated with ongoing and sustainable training programs in the field. Understanding security threats is important for everyone, from end users in end nodes, to cybersecurity professionals and ending with top management at the highest C3 level. In general, the content of the programs and the training process for promoting the desired behaviors is targeted at different target groups with different levels of training (*Fig.1).*

In order to prevent the many cyber risks, social engineering attacks, etc., the masses of users must adopt **scrupulous cyber hygiene**. Cyber-hygiene is especially important for Generation Z children, as their lives are inextricably linked to modern IT and access to Internet-connected equipment, and they are among the most vulnerable to online threats, cyber harassment. Modern children cannot imagine their lives without the Internet and gadgets. They master new technologies much faster than adults and use cybersecurity resources more confidently. Such trust, combined with a lack of life experience for decent filtering, often causes problems for children. Because with the development of the Internet, the illegal, unwritten, unreviewed content grows; cases of aggressive behavior of some users towards others and cyber harassment are becoming more frequent; many children become victims of scams and malware, etc.

Above all, cyber hygiene is a matter of individual responsibility for everyone. All users need to know and apply a number of best practices, both at home and at work. Cyber-hygiene refers to the actions and methods that users of computers and any other electronic devices connected to the Internet must follow to protect personal and corporate data. Cyber-hygiene also refers to the ethics of online communication. This education is dedicated, in particular, to the safe operation of devices in the digital educational environment and must be supported by both the school, the state and the family. Organizations must also adopt and enforce cyber hygiene rules designed to minimize human risk with technical solutions.

Actions to raise awareness of cyber hygiene can range from thematic information campaigns, launched in the form of symposia, conferences, exhibitions, to the publication of newsletters and news on risks in the field of CS and other profile materials on corporate sites, and/or government. At the state level, cyber-hygiene is promoted through strategies, familiarization programs, global orientations, etc.

For example, "Cybersecurity guidelines for eastern partner countries" https://eufordigital.eu/library/cybersecurity-guidelines-for-the-eastern-partner-countries/ published in 2020 by EU4Digital, explores the main obstacles and gaps to be addressed, as well as key challenges and recommendations for strengthening cyber resilience in each of the Eastern Partnership Countries.

CS awareness from TreeTop security (https://www.treetopsecurity.com/cat/), distributed free of charge, "Basic rules of information security" (https://cybereducation.org/mc/index.php/usr/login/login), free course thanks to a grant from CRDF Global, funded by the USA. CS Learning Hub, (https://www.weforum.org/projects/cybersecurity-learning-hub), an initiative led by Salesforce

(https://trailhead.salesforce.com/cybersecurity) with the support of Fortinet, Global Cyber-Alliance and World Economic Forum, Canadian Center for CS, Learning Hub (https://cyber.gc.ca/en/learning-hub/), provides on-demand Cybersecurity skills training.

ABSA Group (formerly Barclays Africa Group) (https://www.weforum.org/organizations/barclays-africa-group-limited), in collaboration with the Maharishi Institute, is successfully running cybersecurity academies, targeting some of the most disadvantaged groups in South Africa.

There are also paid courses, e.g.: Cybersecurity course for children aged 6 to 14 at CODDY (https://coddyschool.com/courses/kiberbezopasnost), Cybersecurity and digital literacy for children aged 11 to 17 (https://gb.ru/courses/geek-school/security? tip-course-x9ng = korotkiy-course) and others, who share their knowledge, security rules, help them protect their personal data and increase their resistance to scammers and criminals.

In recent years, the awareness of the general public regarding Cybersecurity risks has begun to take shape in the Republic of Moldova. The main promoter of the CS is the Public Enterprise Information Technology and Cybersecurity Service (PEITCS), in 2020 designated as the Government Computer Emergency Response Team (CERT Gov MD). PEITCS is involved in several awareness-raising activities through the organization of various international conferences, the publication of reports, the organization of expert workshops, cooperation with international partners, the development of public-private partnerships, the publication of simple cyber hygiene rules (https://stisc.gov.md/ro/reguli-de-igiena-cibernetica-pe-timp-de-covid-19), the publication of the weekly news on CS (https://stisc.gov.md/ro/noutatile-saptamanii-din-cybersecurity-28012022, https://stisc.gov.md/ro/cisa-adaugat-17-vulnerabilitati-catalogul-de-vulnerabilitati-existentecunoscute-si-exploatate) etc.

There are other structures involved, e.g., the State Chancellery publishes and promotes various materials, posters on the increase of cyber hygiene, the Institute for the Development of the Information Society to ensure the continuity of research activities and increase the visibility of scientific results (https://idsi.md/implementarea-cerintelor-minime-securitate-cibernetica-necessara-pentru-organizacións-de-cercetare-inovare), etc.

The main objective of these organizations, programs, international and national events is to create platforms for public-private dialogue, offering the possibility of identifying effective solutions aimed at reducing the risks of cybersecurity, as well as developing strategic partnerships between the public and private sectors and international collaboration on CS issues.

2.3 The continuous growth of the corporate culture of cybersecurity

Management uses security policies as a way of defining what is expected of its members. This assumes that all staff of organization must be proficient regarding this role in the insurance of CS. Maintaining the required levels of competence or raising the awareness of employees is achieved either through initial and in-service training or through specific corporate training oriented at target user groups. And the corporate training aims to create a correct attitude towards CS, in line with the user's position/role in the organizational structure by adopting preventive and proactive measures, based on knowledge of how to manage IT resources and threats towards them.

In order to recruit and develop the right employees in the right places and to maintain the appropriate skill levels, organizations have to be able to understand the areas of CS needed for the different roles. And in order to reduce the gap between academic training and the concrete needs of some entities in mitigating the consequences of cyber threats, each organization should conduct ongoing corporate training according to individual programs, tailored to needs, through various seminars,

trainings, round tables and special cybersecurity courses, including outsourced. For more details see [3].

Organizations must ensure that interested/ responsible information security stakeholders understand security policies and procedures for valuable information assets and comply with the specified conduct rules for the systems and applications to which they have access. Corporations often set up training centers for the continuous training of their own employees. Typically, the target audience for continuing education programs includes top management, professional CS technical staff, employees, and third parties employed by the organization (e.g., contractors, suppliers). Information security management usually involves a "pyramid structure" of communication with different levels of awareness, training and education, which are determined by the internal requirements of the organization and external factors.

At the lowest, basic level of the pyramid, with billions of users, as well as on level 2 *(Fig.1),* Awareness-literacy programs are required, aimed at stimulating security behaviors, motivating stakeholders to recognize security concerns and respond to them.

On the 3rd level of the pyramid, the training programs relate to functional responsibilities in the protection of employees' personal data, in recruitment, integration and termination of employment, the production of security skills and competences, such as the operation of physical and logical security controls.

At the highest level of the pyramid, education aims to develop expertise in the field of information security and is addressed to professionals in CS.

However, computer users, local and global networks, information and communication technologies/systems, Cloud Computing, the Internet of Things (IoT, IoB), etc., do not always succeed in complying with these policies. In order to address this issue and meet regulatory requirements, entities should systematically conduct specific information security/CS awareness programs that address specific key components of the CS for those specific contexts.

There are many eLearning programs from Infosequre (https://www.infosequre.com), SANS (www.sans.org), Quick Start (https://www.quickstart.com/find-training/training-by-topic/information-security.html) etc., which offers a variety of highly customizable security training and security awareness solutions and programs that fit the requirements of any company, including courses, summer schools, training camps, and more.

Basic training and professional certifications in the field of security

If cyber hygiene is a general requirement prescribed, but poorly verified (proven), for certain target groups of professionals in important areas of security, knowledge and skills are validated by certification. Usually, professional skills are obtained through in-depth formal training in higher education institutions and/or especially in colleges and universities, including in designated centers and/or through personalized corporate training programs.

Basic training/formal training is carried out in education at all levels, taking into account the national specifics, the particularities of the digital economy and culture. But this subject is not the subject of present paper. Here we just mention that things have started well in Moldova as well. For example, in an international project ERASMUS + "LMPI Professional Bachelor and Master Degrees for Development, Administration, Management, Protection of Computer Systems and Networks in Companies", carried out with EU support in the period 2016-2019 in some universities, which have opened dozens of new courses related to Information security, CS, Network security, etc.

An ideal tool to support educational institutions, vocational training centers and any organization interested in CS, is the European IT Competence Framework with eCF Explorer (https://ecfexplorer.itprofessionalism.org/). eCF

can be used by anyone, either for the development of specific certification programs in the field of CS, or as a coherent standard of competences to evaluate the existing individual training programs in order to complete them.

The certification of staff demonstrates that the person is qualified as a professional recognized in the area in accordance with certain reference standards, administered by many independent centers and specialized certification bodies. As a rule, certificates demonstrate competencies in a particular field, at different levels, *e.g. beginner, associate, practitioner, professional, expert, architect*; in some specializations, *e.g. management, engineering, audit, firewall, intrusion preventing systems*; in a particular technology, *e.g. Microsoft, CISCO, Linux;* in a certain standard, e.g. ISO/IEC 27001, COBIT 2019 framework *(Control Objectives for Information and Related Technology)* from ISACA, PCI DSS (Payment Card Industry Data Security Standard) from PCI Security Standards Council etc., have a relatively short period of validity *(1-4 years),* or require annual reconfirmation in the form of simplified examinations.

The best information security certificates for security professionals include:

CISSP *(Certified Information Systems Security Professional)*, CAP *(Certification and Accreditation Professional)*, SSCP *(Systems Security Certified Practitioner)* etc. of the International Information Systems Security Certification Consortium (ISC)², founded in 1989 in USA*(www.isc2.org)***,** who developed the *"CBK-Common Body of Knowledge",* a comprehensive framework of all the relevant subjects a security professional should be familiar with, including skills, techniques and best practices.

CISA *(The Certified Information Systems Auditor),* CISM *(The Certified Information Security Manager),* CGEIT *(Certified in the Governance of Enterprise IT)* ***etc.*** of the professional association ISACA.

SANS Institute (*SysAdmin, Audit, Networking and Security, www.sans.org),* founded in 1964 as a research and education organization, seems to be the largest source of information for information security training, which created the CIAG certification program *(www.giac.org, Global Information Assurance Certification)* which offers dozens of professional certifications, as GIAC Security Essentials Certification (*GSEC)*, GIAC Certified Firewall Analyst *(GCFW)*, GIAC Certified Windows/UNIX Security Administrator *(GCWN/GCUX)*, GIAC Secure Software Programmer *(GSSP-C/Java/NET)*, GIAC Systems and Network Auditor *(GSNA),* GIAC Certified Penetration Tester (*GPEN)* etc.

The International Council of Electronic Commerce Consultants, Founded in 2001, *(www.eccouncil.org/)*, a professional organization that aims to develop e-commerce, set professional standards, education and certification, offers dozens of professional certifications as well Certified Ethical Hacker *(CEH),* Certified EC-Council Instructor *(CEI),* Computer Hacking Forensic Investigator *(CHFI)*, EC-Council Certified Security Analyst *(ECSA),* Certified Network Defense Architect *(CNDA*), Licensed Penetration Tester *(LPT)* etc.

Cisco Systems *(https://edu-cisco.org/)*, one of the world's largest high-tech companies, founded in 1984, San Francisco, California, USA, offer such certificates as Cisco Certified Security Professional (*CCSP)*, The Cisco Certified Internetwork Expert Security *(CCIE Security),* Cisco Certified Network Associate *(CCNA)* Security Certification, Cisco Certified Network Professional Security *(CCNP Security),* Cisco Adaptive Security Appliance Software (*CISCO ASA)* etc. (https://www.cisco.com/c/en/us/training-events/training-certifications.html).

For more information on Cybersecurity Training and Courses see https://www.educba.com/software-development/courses/cyber-security-course/?btnz=edu-blg-inline-banner1/, free course

"Ethical Hacking for Beginners" (the fundamentals of ethical hacking) https://www.simplilearn.com/learn-ethical-hacking-online-free-course-skillup?utm_source=frs&utm_medium=skillup-course-banner&utm_campaign=frs-skillup-course-promotion/, free course "Introduction to Cyber Security" (the basics of cybersecurity) https://www.simplilearn.com/learn-ethical-hacking-online-free-course-skillup?utm_source=frs&utm_medium=skillup-course-banner&utm_campaign=frs-skillup-course-promotion/ etc.

According to Cybersecurity Ventures the number of vacancies in CS has increased by 350% in the last 8 years (https://cybersecurityventures. com/jobs) and the 2021 Cyber Security Workforce Survey (SAI) 2 (https://www.isc2.org/-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx) estimates that another 2.7 million cybersecurity professionals are needed.

Choosing the right training techniques

Individuals are often likely to overestimate their own control over the threat and underestimate the chances of the threat materializing. Many people believe that having an IT department or the best security technologies can give them 100% protection. Therefore, simply informing them about the likelihood and potential impact of a threat is not enough; users need to be aware of the risks, know and be able to work safely. Because individual beliefs and illusions affect users' intentions to comply with CS policies, they must be identified and rigorously managed to comply with the rules.

Starting from this premise, educating security behavior involves not only simply knowing security policies and rules, not only understanding of the importance of CS, but also influencing how users perceive risks and make security decisions, taking into account how individuals obtain and process CS awareness information. Awareness programs must be personalized according to the internal/external contexts and business needs of the organization and be relevant to its information culture and IT architecture. This leads us to the idea of the correct selection of the appropriate forms of corporate education of the CS for each of the different target groups of users,

The main techniques of education and sustainable training in the field of CS

Corporate training in the field of CS can be done through lectures, seminars/webinars, trainings and/or workshops *(Fig.3)*. In order to choose the most appropriate option in each case, the purpose and characteristics of each of these forms of education and training should be known. Improperly organized training can be a waste of time and money. And if the training is well planned, it becomes valuable enough for everyone involved.

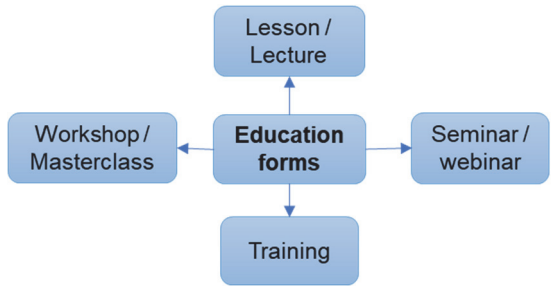

Figure 3. Forms of training

According to the renowned expert in educational psychology William Glasser: *"Man usually learns 10% of what he reads; 20% of what he hears; 30% of what he sees; 50% of what they hear and see; 70% of what they discuss with others; 80% of one's own experience (what one does alone); 95% of what others teach"*

*(*http://thinkexist.com/quotes/william_glasser*)*.

Lesson/lecture is a monologue, a presentation of the provider with minimal interactivity. As a rule, the lecture has an increased volume of information, is aimed at relatively large audiences, can be conducted in any form, with presence, remote/online, including in the form of web-conferences, can be audio/video recorded and multiple repeated/broadcast without losing its meaning. The big problem is that the rate of assimilation of the material of a lecture is quite low,

according to experts at best "about 20% of what they hear".

A seminar/webinar is an extensive and detailed presentation on a relatively narrow topic, involves interactivity and communication between the presenter and a smaller audience, can be conducted in the form of presence or distance/online. Due to the relatively small amount of information and the higher number of transmission channels (sound, graphics, video, interaction), the quality of material assimilation is higher than in a lecture, up to *"50% from what he hears and sees"*. In pandemic conditions, webinars and web-conferences are gaining ground in the face of traditional lectures and seminars, being widely used in all fields and offering large openings of space, audience and space size, which can be virtually any depending on the purpose. At the same time, in addition to the relatively low rate of assimilation in webinars and video conferencing, there are some additional problems such as the need for a high-performance Internet connection, the digital divide, etc.

Training combines mini-lectures, business games, discussions and solving exercises/problems. Due to several mechanisms and stimuli of memory included in the process, the quality of learning and the result obtained is higher, up to "70% of what is discussed with others". Usually, the training removes a person from the so-called "comfort zone", requires certain activities, identifying solutions, etc. and in this way he makes her perceive new things at a high rate. It can last from an hour to a few days, it can usually be conducted in person or, in some cases, in a remote online format, via teleconferencing and interactive tools.

Workshop/masterclass, is quite close to the masterclass. A masterclass is the communication with a master of his craft, and a workshop learns through collaboration; masterclass is a workshop event in which all participants are involved in active group work. Workshops usually involve discussions and the practical application of on-site knowledge. The workshops are characterized by the fact that each participant can "try to do with his own hands" what is being discussed.

Knowledge, Skills, Abilities, Competencies

When we talk about the main techniques/forms of education, we usually refer to lectures, seminars, trainings, as well as their variety: workshops, videoconferences, webinars, etc. But not all and not equally provide knowledge, skills, abilities and competencies, which are closely dependent on each other (Fig. 4).

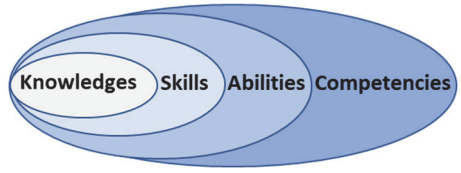

Figure 4. Relationship between Knowledge, Skills, Abilities, Competences

Knowledges are obtained as a result of the process of knowing the surrounding world: of a set of ideas, judgments, theories. Knowledge of CS and cyber hygiene allows users to surf the Internet and operate properly in cyberspace, recognize various common (already known) situations and consciously respond to these events according to best practice recommendations. Professional knowledge of CS is more specific and deeper. They allow the accumulation of Skills - abilities to perform certain actions consciously, based on knowledge and experience.

Professionals must also show certain skills - the ability to perform stereotypical action sets over a long period of time; is when a person repeatedly repeats the same type of actions. Possessing the skills allows you to perform complex tasks much faster and at no additional cost.

The lecture allows to obtain a maximum amount of information in a short time, but the material is poorly absorbed and quickly forgotten. The seminar is good for studying a small amount of material and gaining knowledge on several topics within the topic, it ensures a more active interaction between the speaker and the audience. Training and

instruction in specific masterclasses/workshops are the most effective for the learner and the most difficult for the trainer, they require the active participation and joint work of the trainer and the trainees, their active involvement in the process, which allows the accumulation of experiences own and assimilation up to "*80% of what he does alone"*. Most forms of education only allow the acquisition of knowledge and skills, and for the development of skills and competencies professionals must work on their own. If in a lecture the listener is completely passive, in the seminar he participates to a limited extent in the learning process, then during the trainings and workshops the student immerses himself in a much deeper learning.

Conclusion

Improving users' knowledge and awareness of current and future cyber threats is an essential part of an effective Cybersecurity strategy.

Firstly, because there are about 5 times more technical devices in the world than humans, it is extremely necessary and important to provide effective measures to protect these information assets at the individual level.

Secondly, everything that does not develop - degrades. IT corporate infrastructures, systems and applications, the security measures and policies that protect valuable digital assets are changing rapidly, due of the dynamics of IT and the threats of CS.

As a result, training in the field of CS is a continuum, which begins with awareness, continues with literacy and basic training and evolves towards formal education and professional development professionals. Continuous training in the field of CS is also required by the emergence of new users, new threats, the development of new products, services, technologies and the fact that people forget the acquired knowledge (according to some research, people forget about 70% after 24 hours and about 80% after a month *[9])*.

Thus, the effective management of CS is largely associated with awareness and lifelong learning, the role of which is to get users to comply with information security policies. And maintaining a sustainable CS culture is only possible through a continuous process of raising awareness, updating, measuring, evaluating and cyclically repeating training. Continuous training in the field of CS requires different programs, courses and frequent training and education sessions, depending on regulations, responsibilities, target group of users, specific context, etc.

As cyberattacks become more frequent and violent, governments, public institutions, organizations have a responsibility to protect their dynamic cyberspace. These are the necessities of information security, and understanding of technologies and security threats is essential for everyone, from cybersecurity professionals, governors and managers at any C1-C3 level, and ending with the broadest masses of terminal device users. High management is the one that values security in all types of security: IT/IS information security, security, cybernetics, etc.

Given the dynamics of IT development and the continuous expansion of CS threats, sustainable and continuous training in the field of CS becomes indisputable and without alternatives. This allows for risk awareness, the development of personal and corporate cyber hygiene skills and culture through information, formal, informal, non-formal training and ongoing guidance of target groups, or in generic, free, open and accessible programs for the broadest masses of users. , either as part of corporate continuing education or as part of special certification courses.

In order to be aware of what is happening - it is necessary to follow the news in the field of information security, the emergence of new threats and recommendations of CS. In essence, technology and law are not enough. People are the biggest weakness in ICT systems and. Therefore, cyber security is also based on user awareness and training. Users need to adopt good practices and become as vigilant in cyberspace as they are on the streets.

While the human factor is the weakest link in the CS, human intelligence is the best defense against

attacks, whether they come from social engineering, technical defects, management, etc. Improving knowledge and awareness of current and future cyber threats is an essential part of an effective Cybersecurity strategy.

References

All web references cited in the text were accessed/verified on March 6, 2022.

Digital 2021 Global Overview Report. https://datareportal.com/reports/digital-2021-global-overview-report/

15 Alarming Cyber Security Facts and Stats. https://www.cybintsolutions.com/cyber-security-facts-stats/

NIST SP 800-50. Building an Information Technology Security Awareness and Training Program, October 2003, http://csrc.nist.gov/publications/nistpubs/800-50/NIST-SP800-50.pdf/

Bragaru, T. et al. Securitatea informației vis-a-vis de securitatea informațională. In: Studia Universitatis Moldaviae, 2 (122), 2019. Seria "Științe exacte și economice". - p.38-47

ISO/IEC 27000: 2018. IT. Security techniques. Information security management systems, Overview and vocabulary

Bragaru, T. Dezvoltarea și implementarea sistemului de management al securității informației (în baza ISO/IEC 27001). Ghidul participantului și suport de curs pentru instruirea tradițională, online și/sau la distanță. Chisinau, Tipogr "Foxtrot", 2021. -113 p.

ISO/IEC 27001: 2013. IT. Security Techniques. Information security management systems. Requirements

ISO/IEC 27032: 2012. IT. Security Techniques. Guidelines for cybersecurity

Что такое кривая забывания и как помочь студентам запомнить информацию надолго. https://skillbox.ru/media/education/chto-takoe-krivaya-zabyvaniya