EasyChair Preprint

№ 7017

Enhancement of Cyber Awareness for Users in Public Organizations

Violeta Vasileva

November 10, 2021

Enhancement of Cyber Awareness for Users in Public Organizations

Violeta Vasileva[1][0000-0002-0831-5176]

[1] University of Library Studies and Information Technologies Sofia, Bulgaria
violetta.ziv@gmail.com

Abstract. This paper aims to present a methodology for researching the capacity of users in public sector and administration to manage their digital identity and operate in a safe and secure working environment. The methodology is based on a defined survey research targeting personnel and individual users operating in public cyberspace. Based on the analyzed survey results and formed observations, the paper suggests solutions for improving the competences of users in cyberspace and increase their cyber awareness. As a practical implementation of the proposed methodology, the author presents a developed Cyber Awareness portal. Its main purpose is to provide national and international information and resources on cybersecurity and information security, and to be the main point of knowledge access. The portal also provides opportunities to test users' cyber knowledge, participate in public survey related to cyber topics, share and exchange information, opinions and useful practices on cyber incidents and cyber knowledge.

Keywords: Cyber, Awareness, Survey.

1 Introduction

1.1 Background

Several studies have proved that half of data security breaches are caused by errors due to activities of ordinary business users [1]. This contradicts the notion that hackers are the ones behind most breaches. Another key observation, from the study, is that human mistakes lead to more incidents than malicious actions do. That is why the attention should be focused on human factor activities. Moreover, in the current COVID-pandemic situation many users prefer working by the so-called "Work From Home" model. It requires more detailed research for cybersecurity in order to enhance user's cyber awareness and competence. According to ISACA's Covid-19 Study, about 90% of participants believe that an abrupt transition from the place of work to so called "home office" way of working would increase the risk for data privacy and cause problems [2].

A key aspect of the human factor is related to identity management, which is an important element of a cybersecurity system within organizations, both public and private. With regard to the management of digital identity, key issues are security and

privacy. As digital identity has become an increasingly popular attack vector and identity theft is widespread on the web, measures to identify and validate digital identities are crucial for network management and security in the public and private sectors.

1.2 Rationale

In order to reach the above-mentioned aim of this paper, the issue has been explored, from a user's point of view, by applying a survey research methodology. It gave an opportunity to select key research indicators, related to cyber awareness and digital identity. They were explored and analyzed, and then the evaluation criteria were defined. The study is aimed to help users get certain skills when they operate in the cyberspace. The survey was conducted and its results were compiled and examined. These results are used for the development of solutions that would enhance users` cyber awareness, digital competences and help them maintain high level cyber hygiene. Cyber hygiene is related to building user-oriented habits of their security in cyberspace. Cyber hygiene refers to the steps that users of computers and other devices can take to improve their online security and maintain system health [3].

In addition, from organizational point of view, the results are applied to define information security in public administrative structures.

Based on this, a detailed plan for organization and protection of communication and information infrastructure within public organizations is proposed, taking into consideration the human role.

The notion of human factor within cybersecurity systems in public and private organizations leads to one main observation in regard to user awareness within such systems. Based on the survey results, a human-centric perspective for a practical solution is applied by the development of a virtual online space - a website "Cyberawareness". It provides opportunities for active communication between users. They could submit information to the platform, as well as receive information from it. The virtual space of the platform has several functionalities. On one hand, it offers a tool for researching skills and behavior of citizens, verifying their competencies in cyber awareness, and helps them manage their digital identity. On the other hand, it provides cyber awareness resources, access to various free cybersecurity verification tools, information resources, useful information and contacts, opportunities for sharing information related to cyber incidents, etc.

In this way, the platform could strengthen information sharing and improve cybersecurity competence of the workforce and citizens, especially in the sphere of the public sector and the related services.

2 Methodology for improving cyber awareness of users from the public sector when working in cyberspace

2.1 Research method

The research method is based on the evaluation through analysis of collected data. The data which is collected provides information about the users, their occupation, experience and level of excellence. For the purpose of this study, the survey method was selected as the most appropriate one.

The survey examines and analyzes the opinion of a wide range of participants that work in public and administrative structures. It provides an objective overview of the needs and potential areas for improvement in the organization of information infrastructures in those structures.

The preparation of the survey is related to the following technology for work:

- Studying the general theory and technology of organizing and creating a survey;
- Exploring the possibilities for creating questionnaires or online forms with the relevant topics;
- Selection of indicators and definition of criteria for assessment of information needs;
- Development of a questionnaire;
- Organizing and conducting the survey;
- Processing and analysis of the results of the survey;
- Synthesis of the results, development of conclusions, recommendations and lessons for the administrative and management structures of the country;
- Applying the results of the survey to improve information security, defining them as information resources within the package of capabilities they need to implement, the components of the information infrastructure of the cybersecurity system.

2.2 Indicators for the Formation of the Evaluation Criteria

As part of information security, indicators for the formation of criteria for cyber awareness assessment are related to capability building, as follows:

- Application of service-oriented architecture;
- Capability building for monitoring, detection and recognition of cyber threats in the ecosystem, as a part of public administration structure environment;
- Capability building to ensure effective processing and sharing of information related to cyber incidents and threats between departments and users in administrative structures.
- Personally Identifiable Information and Identity Management.

The needs for information security and services of the systems are planned and built in accordance with their taxonomic (classification) grouping. It is a part of the

comprehensive service-oriented approach. The taxonomy (classification) is a hierarchical model consisting of a certain layer of services, including information security.

Also, the capacity building for monitoring cyberspace is related to sharing data in real time through a subsystem for cyber incident detection.

Effective and efficient information sharing and exploitation between existing Security Incident Response Centers in the public sector is related to the development of automated information systems. These systems are designed to collect, process and share information for cybersecurity incidents and to get users aware of preventing such incidents.

In order to manage increased cyber risks and to improve cyber awareness, it is essential for users to counter detected threats, as well as to be capable and adaptable to neutralize new cyber threats generated by some innovative information technologies.

2.3 Evaluation Criteria Definition

The definition of evaluation criteria is based on analysis of the proposed indicators for information security. It can be concluded that the basis for building the information environment should be a service-oriented architecture. That is why the evaluation criteria can be:

- applying a comprehensive service-oriented approach to build up information security;
- capability building for effective information sharing and processing among different organizational units;
- providing abilities to work in a group environment;
- getting specific abilities in order to observe, detect and recognize the environment in cyberspace in real time;
- assessment of the threat and risk level in regard to identity theft.

The set of indicators determined by the cyber awareness capabilities have been suggested to select evaluation criteria for cyber awareness and the information needs, which are the basis that forms the necessary information resources to enhance the users' cyber awareness. They are a prerequisite for the development of the "cyber awareness" information service implemented through a web portal.

A methodology for assessment of the necessary services for cyber awareness and information security has been developed using a survey method. For that purpose, questionnaires have been elaborated in order to conduct a survey online between several different groups of users

Based on a study of cyber awareness level of the users from public administration structures, a methodology has been proposed to improve their competencies when working in cyberspace and in the context of the COVID-19 pandemic through the development of a portal - a website „Cyber Awareness". It implements the information service for cyber awareness. In this way the analysis of the results of the survey is being used in the development of a solution to increase cyber awareness.

The suggested methodology for **researching** cyber awareness of employees and a method for **improving** cyber awareness competencies are presented at Fig. 1.

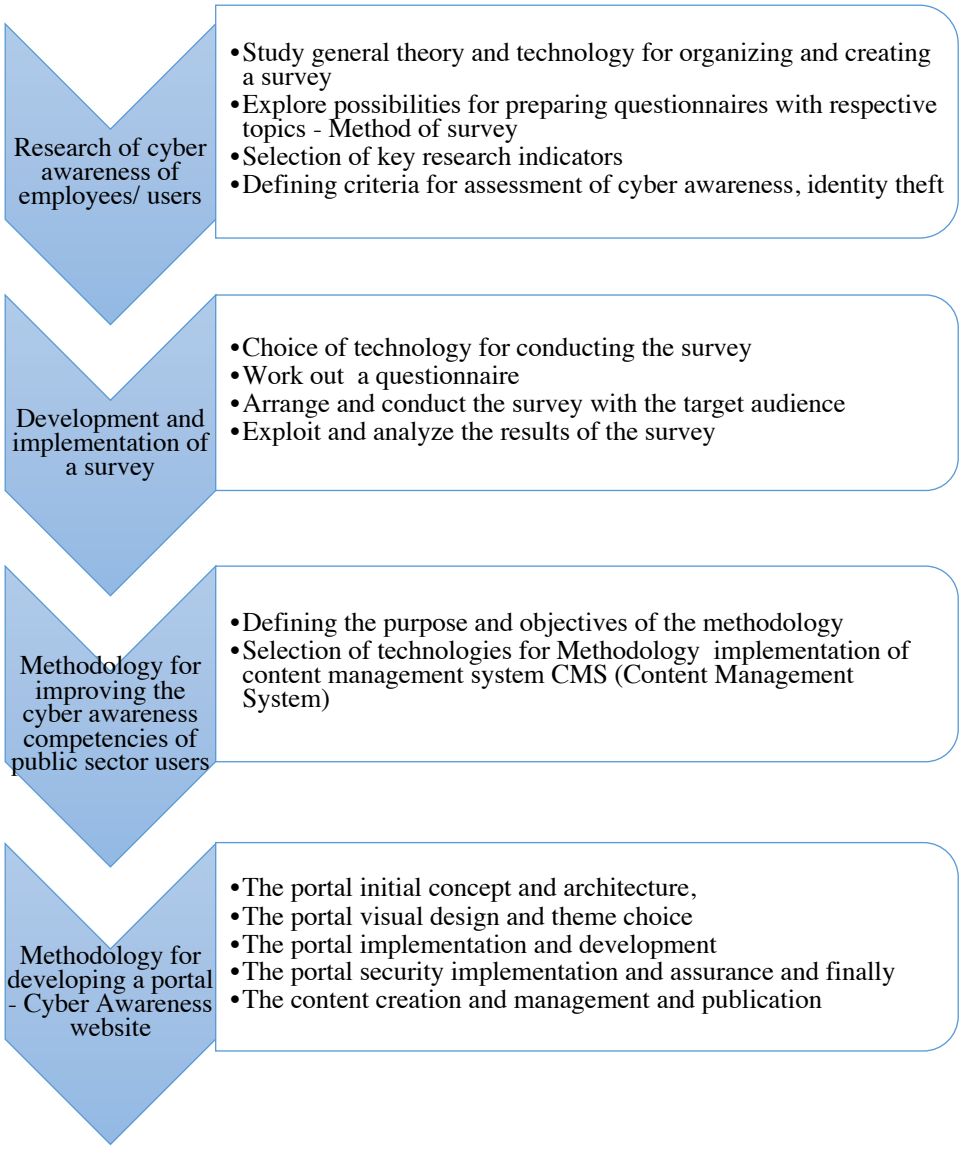

Fig. 1. Methodology for Employee Cyber Awareness Survey and Method for Improving Cyber Awareness Competencies.

And finally, a variant of such a consistent approach for cyber awareness research, identity management, and proposing solution in order to enhance user competencies regarding cyberspace could be successfully applied, both at the national level for one country and for other countries, as well as in an international environment.

3 Results of the Study

3.1 Survey Elaboration and Distribution

Given the dynamic state of information security vulnerabilities and the volume and complexity of existing threats, public organizations face a huge challenge defining and understanding human-related threats and risks. To help understand these challenges, cybersecurity experts and cyber users in public organizations from various institutions were interviewed through a survey. Based on the results of the survey, the key questions that all the users face are related to the lack of information about type of vulnerabilities, risk assessment, risk awareness, access to right information and support.

A questionnaire "Questionnaire to survey the behavior of consumers and institutions in situations at risk of working in cyberspace and in the context of the COVID-19 pandemic" has been developed, which consists of ninety-four questions.

The design of the survey contains three types of questions:

1. Questions with a choice of one answer - the correct answer is marked in the symbol "Radio button".

2. Questions with a choice of more than one answer, the correct answer (s) is marked in the symbol "Check box ".

3. Open questions - free entry of text is allowed.

The survey is anonymous and was developed through the cloud services for online forms and surveys. The “Forms” applications of the Microsoft Teams and Google Forms platforms have been used as implementation technology.

Three different questionnaires (interviews) with the three groups of participants were conducted:

- Group 1: User Level (The survey contains 46 questions out of 94 questions. Up to 90 respondents were sent, 38 answered)
- Group 2: Employees in administrative structures (The survey contains 43 questions out of 94 questions. Questions sent to 179 respondents, 43 answered)
- Group 3: Information Security Specialists (The survey contains 46 questions out of 94 questions. Up to 59 respondents were sent, 15 answered).

Thirty-eight (38) people took part in the survey at the user level respondents. In the second survey, forty-three (43) respondents were interviewed, of which information security specialists were fifteen (15). As the results show, the need for cyber awareness research is not sufficiently recognized. The results show that there are users from all groups who have no interest in participating in the anonymous survey.

Along with the specific answers to the questions, concrete proposals were made. The main one identified the need to provide opportunities for Cyber Awareness. These are opportunities to improve competencies for cyber awareness of users in public sector when working in cyberspace.

3.2 Key Observations

Some key observations are identified as follows:

- More than 50% of participants underwent security training within their organizations (Group 2)
- 78% of respondents say that in the corporations where they work there are established security policies. In a very small part of them these rules are related only to certain activities. Here the role of he leadership is positive and obvious. (Group 2)
- 72% of the respondents would accept when working in cyberspace to comply with the recommendations by observing their own user, monitor their device, knowing their correspondents, use virtual cards for your payments and more. However, 27% would not complied with such recommendations. Although a small percentage of dissenters, yet in a public administrative structure, such percentage is unacceptable. (Group 2)
- Over 60% of employees would like to be involved in training on the implementation of software capabilities to protect information and networks. The training can be done by external training structures, but also by the information security administrators in the organization. (Group 1 & 2)
- The results of the recommendations concern the exclusive administrator on information security. Highly recommended end-user protection and awareness systems. They recommend to have analysis systems in the information infrastructure, incident monitoring and reporting, as well as network sensors. (Group 3)
- More than 50% of the participants recommend the information infrastructure to have cyber threat systems and indicators, along with incident analysis, monitoring and reporting systems. (Group 2)
- More than 50% of the breakthroughs in the networks of corporate structures are due to the human factor of the organization itself and about 30% are caused by external factors and resources. This presupposes prevention in the work of the management with the users in the electronic environment and daily control over the users and the administrators in the network. These conclusions also apply to network administrators for daily work with employees. (Group 3)

3.3 Recommendations

Based on the analysis of the results of the survey the following recommendations could be made towards the work of the users, managers and network and security administrators within public organizations:

Regarding users and managers in institutions. The above data gathered from this group shows that justified cybersecurity concerns are present. This requires the leadership of institutions to develop measures and develop recommendations for safe

work of their employees in the digital (cyber) environment and enhance their cyber awareness.

- About cyber awareness level analysis – public sector organizations should create and use a cybersecurity policy during crises.
- About data analysis, smaller sized organizations with lower budgets and less employees are less prepared and less aware of cybersecurity risks; therefore, more cybersecurity awareness should be emphasized.

Organizational measures are needed, including and those related to identity management as:

Employees need to know that each account matches exactly a particular user and everyone must act responsibly and protect their data. Username information should not be provided and passwords of third parties, as well as in various digital platforms and social media. In case of suspicions about profile theft or compromised account, notify the administrator immediately security in the institution.

Password compromising is one of the main reasons for most cybercrime incidents. Quality management of passwords assume that each account is secured with a unique one access password. Passwords must be sufficient at the same time long and complex enough to be composed of different characters and symbols. Passwords should include words, names or anything that is easy to associate with their owners. In addition, passwords "wear out", i.e. grow old. Each time a password is entered through a keyboard or screen of a device suggests compromising this password. This goes in line with the fact that passwords must be changed periodically.

Improper password management can lead to significant risks of theft and irreversible loss of information, leakage of sensitive data, breakthrough in information systems.

Passwords are strictly personal and on no occasion and under no circumstances circumstance should not be shared with third parties. They are considered top secret information.

Under no circumstances should passwords be sent by e-mail, be recorded on paper, communicated by telephone, fax or other insecure or easy to read format or channel, and under no circumstances should be entered in electronic surveys. Passwords must not be saved and in a file on a workstation, server, or mobile device in unencrypted view.

In terms of **cyber awareness,** serious attention should be given to attacks type of social engineering, which completely circumvent all technical protection measures taken and exploit the vulnerability of the human factor. Social engineering is method for unauthorized acquisition of information resources and / or user rights without the use of technical means. Social engineering uses mainly psychological methods, namely a person's tendency to trust. Social attacks engineering take place on two levels:

- Physical level are offices, telephones, trash cans, business mail.

- The social engineer can simply enter the workplace, posing as a maintenance person, and to get a custom username and password.

This psychological approach uses well-established methods for persuasion: presenting to someone else, conformism, reference to authoritative figure, distraction or just friendly attitude. The most common and easy way to get a third party with username and password is by receiving it directly from the user through various methods of persuasion, deception, involuntary sharing, misleading in order to achieve financial benefits, etc. Social engineering is the preferred method to launch an attack on a system because in case of carelessness on the part of the user the attacker can easily obtain the necessary information.

Summarizing the Internet user must comply the following rules:

1. Not to give personal information: name, address, password from e-mail mail, social network profile, personal phone number, institution of work.

2. Not to give information about the place of work or personal and official phone number of relatives, friends and acquaintances without their permission.

3. Not to send or upload my photos and videos online.

4. Do not send or upload online photos and videos to friends, relatives, relatives, acquaintances, etc., without having previously discussed with hem, and in the case of friends and colleagues, to be agreed with them.

5. Do not reply and do not open digital attachments in mail received from an unknown sender. It may contain a virus or another malware that can damage computer / phone / tablet or made it vulnerable to external access.

6. Consult a specialist before downloading or installing new program / application on computer, phone, tablet, and avoid actions that could damage the computer or that could reveal personal and professional data.

7. Personal Internet activity should not harm my work me or to contradict the established rules, some of which are regulated by law.

8. It is forbidden to use someone else's username, password and email.

9. Do not write or upload anything that may be offensive or humiliating for you or your collages.

12. Use difficult (long, uppercase and lowercase letters, numbers and special characters) and different passwords for each site.

13. Use an antivirus program that follows regularly updates. Together with the network administrator maintain the latter updated versions of all programs and applications.

20. In case of using shared computers, always check if the user is logged out after logging out of personal account. In case of finding a device that someone else has worked on but hasn't closed their account, log out immediately without viewing, changing or adding information in their profile.

Adherence to these rules will ensure relatively safe working environment for it`s users operating in the cyber space. Administrators should also be committed to complying with the network and security rules, as well as the management of the institution`s information infrastructure.

3.4 Developing the Project Portal "Cyber Awareness"

In line with the observations based on survey results, the author presents a methodology for enhancing the knowledge of public sector organizations` personnel to work in a secure environment and to refine and improve their cyber awareness skills. As a practical implementation of the proposed methodology, the author presents a developed by her Cyber Awareness portal. Its main purpose is to provide national and international information and resources on cybersecurity and information security, and to be the main point of knowledge access. The portal also provides opportunities to test your cyber knowledge, participate in public survey related to cyber topics, share and exchange information, opinions and useful practices on cyber incidents and cyber knowledge.

Portal design and development. The project for the portal design and development has followed a waterfall approach, where a breakdown of project activities is done into linear sequential phases. The main phases through which the project underwent are as follows:

- The portal initial concept and architecture,
- The portal visual design and theme choice,
- The portal implementation and development,
- The portal security implementation and assurance
- The Content creation, management, and publication

Portal Concept and Architecture. In the initial phase of portal planning, the goals, idea, concept and architecture of the topic and activity of the initial website are specified, as well as the information structure. They determine what to expect and get as a result after its completion, in terms of structure, functionality. For this purpose, as a useful practice, it is proposed to develop a site map describing menus, pages and brief content using Excel. The following Table 1 gives a summary of the site map.

Table 1. Site map.

URL: https://cyberhelp.digital/ Aim: cyber awareness platform					
Menu :	**About us**	**Useful information**	**News**	**Cyber-tests**	**Contacts**
Explanation	page with general information about the purpose of the site	page with general information about the purpose of the site	ability to publish news as a link from other sites with a picture, text and link, as well as add your own.	sections with the possibility of publishing: - Different types of tests to determine the level of cyber knowledge, awareness and functionality of users. - Surveys for the study of cyber awareness indicators. Each section must have a name, title, body and link (and the possibility of a logo or avatar - graphic image)	page with useful links for citizens with state and European institutions
Homepage	This is a virtual space for cyber awareness. Here you can find national and international documents on cybersecurity and information security. The website provides opportunities to test your cyber knowledge, participate in cyber identity surveys and surveys, share and exchange information, opinions and useful practices on cyber incidents. In addition, it provides access to useful tools and resources for checking various information resources in cyberspace, information on events and news, as well as useful links to national and international cyber defense organizational structures.				
design- color -dark black					
Cyber-test section - TITLE Cyberhygiene test BODY: here you can test your cyberhygiene competencies - LINK for test (will be tested					

Specifying the content and collecting information. It is necessary to prepare texts, documents, URLs and other materials. Development of the platform kicked-off with setting up the initial structure in the form of website.

The name of the initial site is also chosen, i.e. **choosing a name and domain**. Choosing a domain for the site is an important condition in the process of creating a website. It is especially important that the domain of the site contains, if possible, an important keyword for it and for the activity of the organization, which will potentially help for better indexing of the site by search engines. The choice of a domain name is closely related to the concept and future user orientation of the site. There are several approaches for choosing a domain name keyword:

- Important keyword for the activity. It is recommended when the emphasis is more on the activity and function that is performed by the site (or organization),
- Organization name for domain name - It is recommended when the emphasis is on the representation of the organization in the web space,
- A combination of a keyword about the activity and the name of the organization, which can be merged or hyphenated between them. It is recommended when both are of equal importance. In this case, it is necessary to consider the length of the domain name. It should not be too large, as this would lead to difficulty remembering and the possibility of an error when typing manually in the address field of the browser or speaking on the phone.

Choosing a domain is also about checking that the selected name is free. In many cases, it turns out that it is already occupied or free, but not with the extension with which the initial choice was made. Therefore, it is advisable to devote time and attention to choosing a suitable domain, as it will not be able to change later.

For the purposes of the proposed methodology and the implemented project for choosing a domain name keyword, the first approach was chosen. The chosen keyword – "cyberhelp" relates to the activity.

As mentioned above, in the initial phase - the website concept and architecture development - the main goal is the creation of the website structure and a mechanism through which the content of the website will be created and managed. After considering the project requirements, namely such that fulfil the project's purpose for provision of relevant and useful information on cybersecurity, the next step is choosing the portal for site development.

Choosing a portal for site development. WordPress as a Content Management System is chosen for the development of the site. There are a couple of main reasons underlying this decision.

Firstly, WordPress is a free open-source content management system. Being open source, the system has a complete set of documentation that allowed the team to develop the website as the project's needs and be flexible in the development.

Secondly, wide application's popularity and gained national and international usage of this portal has been taken into consideration. As of May 2021, according to the stats of W3Techs [4] WordPress has 40% market share of all public facing websites on the Internet. This large market share is due mainly to the ease of use of the system for back-end users (users with administrative rights), as well as several useful features such as integrated content management.

Thirdly, the degree of privacy that the portal provides. WordPress has a five-star privacy rating from the Electronic Frontier Foundation [5]. In addition, the degree of security that the system provides is suitable for the requirements that team set before the development of the project.

Selecting and developing a site design. The next phase of the project is the selection and development of the visual design of the website and the choice of WordPress theme. This includes defining: User interface; Site structure; Navigation and Design.

In WordPress, themes are a set of templates that visualize the content for public users. In WordPress there is a wide variety of themes, which are a set of templates that visualize for users the content of the site with a certain graphic design, color scheme, as well as the appropriate arrangement of objects on web pages. When considering what visuals should be used, the team decided on using latest design trends concerning User Experience and User Interface. Solemn, but modern and avoiding clichés color scheme was chosen to reflect the nature of the website as Cybersecurity is a very serious topic. Modern User Experience trends are reflected as micro-animations are used to enhance public users' experience when browsing the website.

Moreover, the de-facto standard industry approach for "mobile-first" design means it is easily accessible from any device, including mobile and tablet devices, as well as

the traditional laptop and desktop devices. The frontend of the website is also compatible with the latest three versions of all major browsers.

Regarding the visualization of browsers on mobile devices [6], it is necessary to apply the following good practice: the pages and links on the site should be located in separate sections of the site main menu only in the "drop-down" menus. If there were "cascading" menus and submenus, this would make it difficult to navigate the pages through a browser on a mobile device or tablet.

WordPress deployment - environment and the website installation and setup. The next phase of the project was the actual WordPress deployment, installation of the chosen WordPress, implementation of various functionalities specified as per the project's requirements and any additional development activities. Overall, this phase process included:

- Initial setup of the WordPress;
- Subsequent implementation of modules (plugins) for various functionalities that were set in the initial plan for the website (e.g., modules for contact forms, visual content management and editing, security management, backup management, multilingual version creation);
- Implementation of a WordPress theme for visualization. The theme name is Ivory. It is a theme that was purchased under license for the use of the website. In order to customize the theme to accommodate the project needs and requirements best industry practices were applied;
- Content input and layout.

Security implementation and assurance. The next phase of the project focuses on the implementation of security measures to ensure the required level of website protection. A set of actions were undertaken in order to assure that the website is secured for a variety of threats. It includes, but is not limited to, the following key measures:

- Implementation of a specialized WordPress module (plugin) for security.
- Server setup for prevention of commonly known attacks against WordPress based systems, as per the Open Web Application Security Project Top 10 list [7]. Some potential threats include Cross-Site Scripting XSS, Clickjacking and others.
- Implementation of server Security Content Policy to restrict the types of files and content served to end users.
- Implementation of Let's Encrypt SSL certificates to ensure secure connection between the website's server and end users. Let's Encrypt is a free, automated, and open certificate authority brought by the nonprofit Internet Security Research Group [8].
- Implementation and configuration of Cloudflare Web Application Firewall to ensure proper mitigation of potential Distributed Denial of Service attacks and filtering of malicious traffic.

Content creation, management, and publication. The final phase of the project was the content creation, input to the WordPress panel and management. The website content is bilingual – English and Bulgarian. It provides potential users information in

their language. Content is broken down to different sections, relevant to different aspects of Cybersecurity.

Publishing to a web server. The content of the website is entered into the selected server and is published on the Internet.

A file transfer protocol (ftp) is commonly used to transfer files to the Internet. There are several free ftp clients on the Internet that can be installed. The website is located at the following URL – https://cyberhelp.digital and is hosted Bulgaria.

4 Conclusion

Digital technologies became everyday commodities, peculating both our social and work environment. Complexity, variety and frequency of cyber incidents has increased significantly over the last decade. Understanding cybersecurity risk requires certain level of discipline and cautious mentality, which requires increasing cyber awareness levels among regular users in both public and private organizations.

The developed portal under this study is a best practice which can be further improved in a collaborative platform that enables regular editing and enrichment of the content with additional up-to-date information, setting up a forum and discussion structure, as well as adding additional tools for site checking and analyzing such as statistical site traffic, number of documents downloaded from it, links of other organizations to it and others. The proposed methodology for improving cyber awareness of public sector employees has an interdisciplinary effect, as it could be successfully applied in other cyber domains and areas of cyberspace.

References

1. 2018 IT Risks Report, Netwrix Corporation, https://www.netwrix.com/2018itrisksreport.html, last accessed 2021/10/19.
2. ISACA's COVID-19 Study, April 2020, https://www.isaca.org/go/covid19-study, last accessed 2021/10/19.
3. Good cyber hygiene habits to help you stay safe online, AO Kaspersky Lab., https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits, last accessed 2021/10/19.
4. W3Techs - World Wide Web Technology Surveys, Usage statistics and market share of WordPress, https://w3techs.com/technologies/details/cm-wordpress, last accessed 2021/10/19.
5. Reitmanjuly R., Who Has Your Back? Government Data Requests 2017, Whitepaper, july 10, 2017, https://www.eff.org/who-has-your-back-2017, last accessed 2021/10/19.
6. Peteva, Irena & Denchev, Stoyan & Tsvetkova, Elisaveta. (2020). Mobile Technologies in Support of Education and Library Provision, ICERI2020 Proceedings 2423-2430. 10.21125/iceri.2020.0577, https://library.iated.org/view/PETEVA2020MOB, last accessed 2021/10/19.
7. OWASP Top Ten, https://owasp.org/www-project-top-ten, last accessed 2021/10/19.
8. Let's Encrypt Homepage, https://letsencrypt.org/, last accessed 2021/10/19.