Information & Security: An International Journal

Predrag Tasevski, v.34:1, 2016, 7-22 https://doi.org/10.11610/isij.3401

IT AND CYBER SECURITY AWARENESS-RAISING CAMPAIGNS

Predrag TASEVSKI

Abstract: Usage of technology in Macedonia has drastically expanded over the last decade. At the same time, it introduces new risks and threats to the country in cyber space. To react against those challenges in the country, there are couple of awareness-raising campaigns, brought by government and non-government actors. However, the existing campaigns are only targeting children, parents and teachers, and institutional level and privacy concerns, while forgetting the end-user. Mainly the approach, in which the awareness campaigns are designed, relies on posters, guides, tips, websites, caravans, etc. For this reason, the article briefly analyses the Macedonian IT and cyber security awareness campaigns, coupled with the background of cyber security path about IT and cyber security awareness-raising. It suggests recommendations and solutions that should be considered in order to raise the awareness level in order to provide safer, more secure and trustworthy cyber space at all levels.

Keywords: awareness, cyber security, IT security, privacy, campaigns, cyber security culture, awareness-raising.

Introduction

Awareness is the first line of defence for the security of information systems and networks. Therefore, the Macedonian government together with the society (represented for example by non-governmental organizations (NGOs), non-profit organizations (NPOs), universities and private companies) are promoting IT, cyber security awareness and privacy campaigns in the country. On one hand, raising awareness among all actors and stakeholders is fundamental and yet not sufficient to fight against cybercrime, while on the other hand it is important to promote privacy concerns and awareness by providing security good practices to vulnerable groups. Such vulnerable groups are: employees in organizations, government, financial, private companies; parents and guardians; children and youth, etc. For this reason, the main idea of an awareness campaigns is to promote a culture of cyber security that will address the entire population needs.

Right now, many organizations, countries and schools implement different approaches to increase the level of awareness. For example, one approach is to issue guidelines to provide practical awareness advice to public and private organizations; it is implemented by the Organisation for Economic Co-operation and Development (OECD) where main focus is in the form of guideline that each participants taking part in campaigns should be aware of the need for security of information systems and networks and what they can do to enhance security.[1] Moreover, European Network and Information Security Agency (ENISA) develops users' guide document that aims at providing practical and effective advice to public and private organisations allowing the reader to prepare and implement information security awareness initiatives that apply to them.[2] Additionally, the National Institute of Standards and Technology (NIST) published a detailed guidance on designing, developing, implementing, and maintaining awareness and training program within an agency's IT security program.[3] Also, the United Nations (UN) Group of Governmental Experts and the Confidence Building Measures (CBM), published by the Organization for Security and Co-operation in Europe (OSCE), recommends situational awareness data sharing for transparency and confidence-building measures in outer space activities.[4]

Despite the international organization approaches, yet there are alternatives, for instance designing an application or interactive videos to promote awareness, or training, brochures, visual websites, and so on. We can make a preliminary conclusion that there are enormous amounts of guidelines, documents and various approaches regarding awareness, with different goals and underlying methods.

Macedonia it is a country that in recent years has been growing rapidly, in particular as regards telecommunications and of the information society. The usage of Information and Communication Technologies (ICT) increases significantly depict by the State Statistical Office for 2015; particularly 69.4% of households have Internet access, while for enterprises with 10 or more employees the figure is 93.5%. Another significant figure is that Internet connectivity via mobile broadband connection is growing, too.[5]

Moreover, since 2009 the government pursues a national program called e-Macedonia within preliminary goals being: *e-education, e-citizens, e-business, infrastructure, e-government and Information Security*.[6] These developments add value to the economic and social status, as well as they expose both state and non-state actors to a potential cyber risk.

Such development and growing usage of ICT leave no doubt that country must somehow improve their IT and cyber security culture and capabilities. Even though the government has spent millions on securing the infrastructure, all it takes is one employee clicking on one wrong link to compromise critical data and information sys-

tems. Consequently, end-users' security awareness is in fact a major issue in the national, organizational and social aspect in world today. Likewise, the threat landscape is complicated, and many end-user are not aware of the ways in which they could adversely affect their personal wellbeing, their organization or the state. For this reason, a holistic approach should be taken into consideration in developing a cyber security culture and increasing awareness by seeing to boost the awareness in the weakest link in security, which is the human factor.[7]

Based on the above information, this article first discusses the government strategy and activities that are underway in respect to raising awareness. Then it provides an analysis of the campaigns and activities developed by the NGOs, NPOs and schools. Last but not least, the article highlights some recommendations on how the Macedonian cyber and IT security awareness should develop and tailor in protecting the weakest link. Furthermore, we depict analysis results carried out in secondary schools in the capital city. Finally, the article concludes by listing what is in the focus in awareness campaigns in Macedonia and provides recommendations.

Background

Looking long-term, in the middle of 2014 the Macedonian government is moving forward in the establishment of a national body, which will play the role of a responsive team that will deal with computer incidents, namely the Macedonian Computer Incident Response Team (MKD-CIRT).[8] It followed ideas which have been under discussion since 2012, and the body was formed officially. The official release came in the country's progress report from European Commission for 2015.[9]

However, some neighbouring countries are lacking such teams, for instance Serbia and Kosovo.[10] Yet we have to underline that Macedonian activities towards awareness are less advanced and progressing more slowly than in some neighbouring countries, such as Bulgaria, Greece, and Albania. Needless to say, this article draws more focus to the awareness-related activities which are on the way from the following body, a part of its reactive and proactive services. The national body will be in charge of raising public awareness of the importance of information security, and conducting educational trainings for specific user target groups. And it will provide support to build a national culture of information security for raising awareness among users and citizens, as noted by former minister Ivo Ivanovski.[11]

The MKD-CIRT team is a part of the Agency for Electronic Communications (AEC). The team provides proactive services on announcements and basic awareness, as well as education and training, while on security quality they pursue on advanced awareness, education and training.

Unfortunately, the observation is that the national body takes under control only the basic and advanced approach to training and awareness education, while lacking the specific targeted audience and collaboration between actors.

Apart from establishing the national body, also in mid-2014 the United Nations Development Programme (UNDP) proposed an assessment study for the requirements for preparation of a National Cyber Security Strategy in Macedonia.[12] Mainly the establishment of such document is under the umbrella by the Ministry of Foreign Affairs [13] and seven different members.[14]

Among the other related national cyber security strategies, the same document highlights that the new body will deal with establishing common standards, training, and education of all institutions involved in the development of cyber security. And it is strengthening the national capacity for prevention and protection against cyber attacks, as well as implementing a campaign to raise cyber attack awareness.

The strategy depicts four segments, such as:

1. developing and promoting the cyber defence concept;
2. measures and activities for cybercrime suppression;
3. establishing and improving a system for preventing cyber attacks;
4. managing incidents caused by cybercrime.

The conclusion is that the strategy itself adds value to the process of drafting and developing a national cyber security strategy in line with the EU's cyber security Strategy and NATO requirements. However, there is still room for improvement. Such potential improvement could be seen for example in Finland's Cyber security Strategy, e.g. in improving the cyber expertise and awareness of all societal actors; improving comprehensive cyber security situation awareness among the key actors that participate in securing the vital functions of society, and establishing active collaboration between actors whose aim is to achieve a shared situation awareness and effective defence against the threats.[15]

The next section of the article discusses the analysis of publicly available campaigns in the light of IT and cyber security awareness in Macedonia and notes the indicators and benchmarks of awareness campaigns.

Analysis

The threat landscape note by ENISA has shown such a wide range of change in the year 2014, for instance increased complexity of attacks, successful internationally coordinated operations of law enforcement and security vendors, but also successful attacks on vital security functions of the Internet.[16] Mainly, the dark side of the threat

landscape of 2014 are the data breaches, vulnerabilities found, privacy violations, etc.[15]

Furthermore, it is important to note when talking about IT and cyber security the difference in regard to goals. In IT security the goal is to protect information from a wide range of threats in order to ensure business/organization continuity, reduce business damages and maximize return on investments (ROI) and business opportunity. Likewise, the aim of cyber security is to protect ICT systems and Critical Infrastructure (CI) and Critical Information Infrastructure (CII). However, the most important protection element in IT security is to reduce business risk to accepted levels and the protection of entire information and information systems essential to the organizations, while cyber security aims at assuring critical IT service for CI and CII on accepted levels. In other words, the security objective determiner in information security is an organization's business process, while in cyber security it is for the entire state. The emphasis is that states might have different or complementary interests compared to an organization's business interests. On one hand, handling cyber security problems is considered to be both a national and international coordinated activity to protect state interests. Similarly, to IT security goals—confidentiality, availability and integrity—in cyber security additional goals are: non-repudiation, authentication, information systems importance and criticality from the standpoint of state CII/CI.[17] Such aspects are vital to understand due to the fact that the main idea in awareness-raising campaigns is to promote a culture of IT and cyber security that will touch the entire population needs; consequently, it is important to promote reforms in legislation and frameworks.

Comparing with the regional countries, Macedonian cyber security culture is progressing slowly. However, we need to keep in mind that this is the case in other countries too, for example Serbia [18] and Bosnia and Herzegovina,[19] which are not so much different of Macedonia in terms of approach and method in awareness-raising. On the other hand, other counties are rapidly progressing, such as Bulgaria,[20,21,22] Albania,[23] and Croatia [24] by delivering not only campaigns, but also implementation into national strategy and education to continuously raise the awareness level into different targeted groups, different levels, emphasis on multi-stakeholder and private public partnership.

That is why in this section the article compares the national state campaigns and those of NGOs and private/school campaigns that are elaborating in increasing awareness level in Macedonia throughout different groups and national agencies (see Table 1). Such campaigns are presented in chronological order:

- Children's Rights on the Internet – Safe and Protected and Online Privacy Made Easy (CRISP);[25]

Table 1: List of campaigns available in Macedonia, organized by different stakeholders and targeted audience by format of implementation.

Campaign name	Organized by	Targeted groups	Format	Language
CRISP	Metamorphosis, EU, and 12 geographically dispersed NGOs	Children, parents and teachers	Website containing: guides, tips, video, games, posters, etc.	Macedonia and Albanian
Surf Safe	Ministry of Information Society and Administration, UNICEF and others	Children and parents	Caravan, posters, guides, and parental control software	Macedonian and Albanian
Privatnost (Privacy)	Metamorphosis in partnership with the Directorate for Personal Data Protection (DPDP)	Any end-user	Website offering analysed law information – data protection	Macedonia, Albanian and English

- Surf Safe;[26]
- Privatnost (Privacy);[27]

Undoubtedly, there are not so many campaigns dealing within such important issue in Macedonia. Yet this article will try to pin-point their value and contribution in increasing the awareness and awareness-raising in the field of IT and cyber security, as well as privacy.

Children's Rights on the Internet – Safe and Protected and Online Privacy Made Easy (CRISP)

The first developed project about awareness-raising on Internet is by Metamorphosis. Metamorphosis is an independent, non-partisan and non-profit foundation based in Skopje. Its mission is to contribute to the development of democracy and increase the quality of life through innovative use and sharing of knowledge. Their guiding values are openness, equality and freedom. Metamorphosis started working in 1999 as part of the e-publishing program of the Foundation Open Society Institute – Macedonia, and became an independent foundation in 2004.[28]

The CRISP project started between October 2007 and November 2008, with the support by European Union (see Figure 1). This project aims at protecting children's rights on the Internet and providing a safe and secure access to the Internet, protection of their privacy and consequently the privacy and security of their families. The project involves a network of 12 geographically dispersed NGOs works on raising awareness and capacity building in primary and secondary schools in Macedonia.

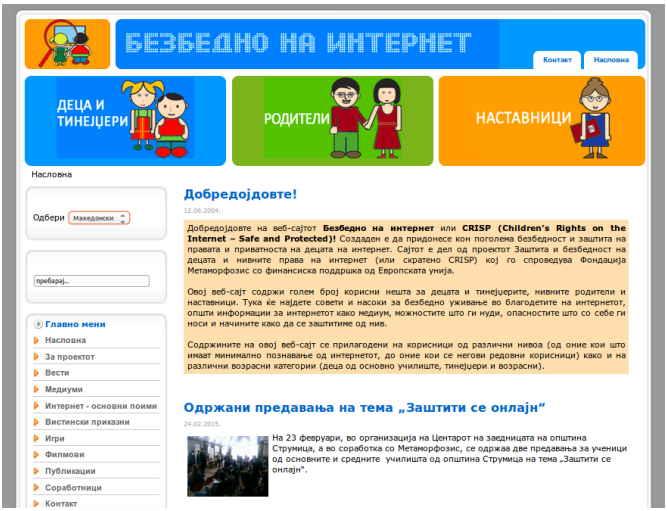

Figure 1: Crisp.org.mk website (in Macedonian language).

Lectures and trainings, provided for the children, parents, teachers and the public, are based on specially developed educational resources in Macedonian and Albanian language, in respect to train the trainer approach.[29]

Along with brochures and posters, the project is publicly and freely available on-line in the form of a website, containing many useful items for children and teenagers, their parents and teachers. Readers could find tips and guidelines for safe enjoyment of the Internet, general information on the Internet as a medium, the opportunities it offers, the associated dangers and ways to protect themselves. Unfortunately, the website is not available in the English language.

The Directorate for Personal Data Protection (DPDP) develops a project similar to the CRISP project, that is focused on games, videos and questionnaires regarding data protection and privacy issues on the Internet.[30] The project is called “Class for Privacy” and its results are further shown in the discussion section of this article.

Moreover, since the very beginning, the project itself draws a big attention regarding the safety on Internet, and from the Sitemeter site summary after applying reverse-engineering techniques it is visible that the project was visited by more than 100,000 visitors and nearly 1 million of pages have been viewed from the region and elsewhere.[31] Noteworthy about the project is the content, which offers basic concepts on Internet, true stories associated with e-mail, on-line chat, social networking and mobile phone usage; it also provides interactive games such as on-line fraud, mobile phone fraud, secure passwords, cyber bullying, etc. Among other things it provides

interactive films, posts, useful tips for children and teenagers, parents and teachers, and a guide which website one should trust.

In short, the following project it is one of the first awareness raising project regarding the safety on Internet and followed by activity such as Online Privacy Made Easy. Therefore, it deserves to pay attention and to acknowledge its outcomes. Finally, each year in February the project delivers a *Safer Internet Day* campaign.[32,33]

Surf Safe

The campaign for safety of children and youth of the Internet "Surf Safe" started in March 2013, promoted by the Ministry of Information Society and Administration together with representatives from other ministries and institutions.[34] In a press conference they noted that the focus of the "Surf Safe" campaign is on understanding the risks and dangers that lure children and young generations on the Internet, as well as recommendations for awareness and recognition. Moreover, the former Minister emphasized that it is important to protect children, by making them aware with whom they talk on the other end of the Internet connection and be aware of fake profiles on social networking sites. Unfortunately, often youngsters end up exploited sexually, by bullying or through pornographic materials.

For this purpose, the government established the Advisory Council with a main goal the protection of children and young generations from sharing and being exploiting on the Internet. The so established council is to develop an action plan and coordinate efforts with a Centre for Safer Internet in accordance with EU standards and create a national strategy for better Internet, as noted former Minister Ivo Ivanovski.[34]

"Surf Safe" is conceived as a travelling caravan within target locations such as primary and secondary schools in the country. The caravan is joined by representatives from UNICEF (The United Nations Children's Fund), the School of Information Technology and Engineering,[35] the Agency for Electronic Communications,[36] and the non-governmental Internet Hotline Provider.[37]

The campaign in form of a caravan provides posters in Macedonian and in Albanian languages in 1,200 copies. Additionally, guidelines for parents, guardians and teachers are distributed in the form of an information leaflets in 120,000 copies. Among posters and leaflets, the campaign distributes software for parental control with activation keys for free. Also, the software is freely available from the web-site shown in Figure 2, however only in Macedonian language.

At the beginning of the campaign and the caravan, private companies, education institutions and the Ministry of Interior also organized one-hour practical training on the topic "I can hack your Facebook, can you catch me ... "[38] Aiming at introducing the

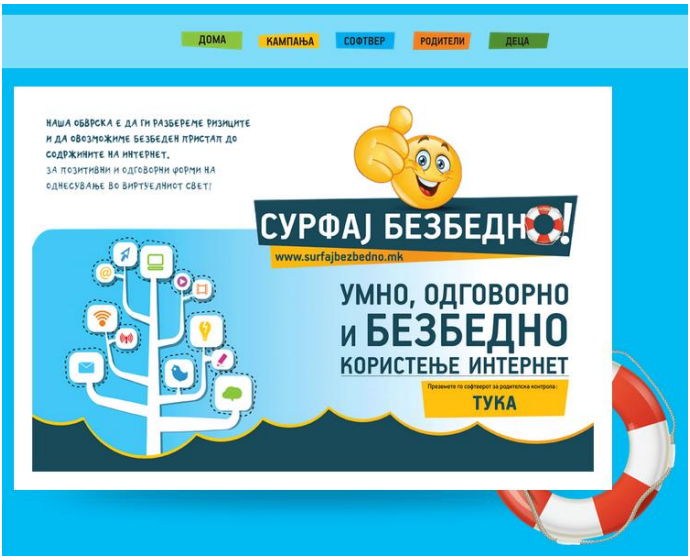

Figure 2: Surfajbezbedno.mk website (in Macedonian language).

possibilities of hacking social networks sites, how you can find and discover an intruder and how to protect yourself in the future. The training was held on May 10, 2013 and it was free of charge to all interest participants, whereas media coverage of the campaign was not so well archived.

To sum up, the following campaign and the caravan have been successful in archiving the goals in increasing the awareness level to the children, parents, guardians and teachers regarding how to surf safe on the Internet.

Privatnost (Privacy)

The Privacy project is a research of the legal and institutional frameworks in Macedonia in terms of privacy aiming to evaluate the current situation and opportunities by analysing frameworks for the protection of citizens' individual privacy.[39] The project starts at the end of 2015 by Metamorphosis in partnership with the Directorate for Personal Data Protection (DPDP) in Macedonia (see Figure 3).

It provides awareness through visual presentation of the analysed laws in Macedonia by emphasising the EU regulations, and is available in three languages: Macedonian, Albanian, and English. The project provides a reference framework and methodology for conducting future researches and projects in this field. Furthermore, identification of laws and bylaws affecting the right to privacy, particularly the ones about regulating and raising the awareness for the personal data collection, processing, transfer and

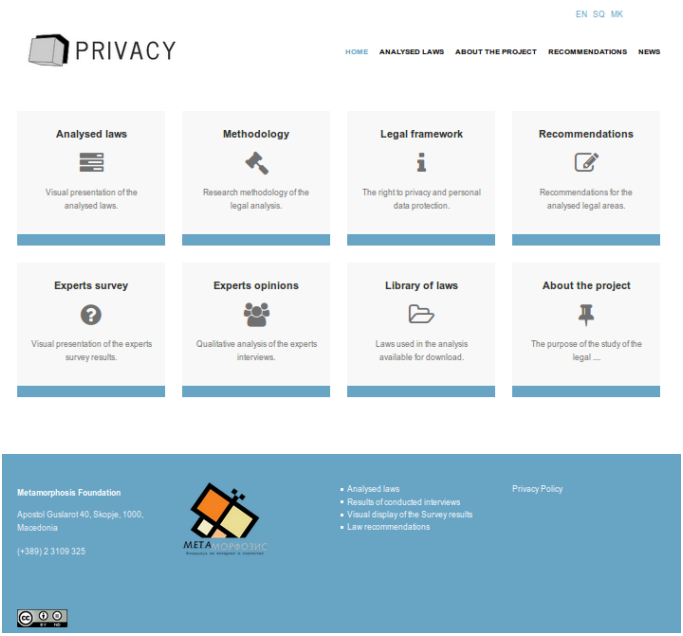

Figure 3: Privatnost.mk website.

storage, with the main goal to help citizens (who are not legal experts) to easily identify the methods, laws and institutions that may compromise their privacy.[39]

In a nutshell, project analysis results in recommendations for various areas and specific laws. Such recommendations are: need for introducing amendments to some of the articles of the analysed laws, or for introducing new articles, where this will guarantee the privacy of the citizens when their personal data is being collected, stored, processed and transferred,[39] and last but not least to provide continuous awareness-raising education from protection of privacy and personal data to end-users.

Discussion

The observation highlights that most of the projects regarding awareness-raising in Macedonia are oriented on pupils and secondary schools' campaigns in respect to privacy, security on Internet, security on mobile phones, etc. Interestingly, this was noted by the research and analysis of responses to the questionnaire for pupils of secondary schools of the city of Skopje – project "Class for Privacy," presented in the beginning of 2015 and on eSociety conference – Freedom and Privacy on the Internet held on December 10, 2015.[40] Main goal of the project is to raise the awareness of

teachers, students and parents in order to prevent exposure on Internet, hate speech, network security, secure passwords, hacking, etc.[41]

Selected participants were from 21 high schools in territory of capital city – Skopje. Total number of participants is 613, whereas 48.3 % are males and 51.7 % females. The participants are between 14 to 18 years old. Needless to highlight is that participants need to be careful regarding personal data to be published without any consent, by fake profile on social networking, abuse of social number, someone spreading hate speech and not to become victims of cyber attacks. This underlines just how important is privacy and security, especially awareness in children, parents and teachers. Last, participants believe that more information about other topics in fact is needed, for instance: increasing security – which sites are not safe; cyber attacks and statistics; hate speech on the Internet; social networking privacy awareness; abuse of personal information; secure usage of mobile phones; etc. Thus, analysis concurred with our initial statements that there is need for a national awareness strategy.

Given that the findings are based on a limited number of participants, and only from the capital city, the results from such analysis should therefore be treated with considerable caution. What is surprising is the fact that such campaigns and programmes are effective in raising awareness level for students, teachers and parents. Presumably, if such research will be carried out in other cities and regions, the results may differ due to the fact that, among the selected age, more likely to have access to Internet and smart mobile phones are students from the capital, compared to those from other, e.g. rural regions. And there is a good probability that such project would be carried out in different cities, different age groups (primary and high schools and universities), as well as in private and government organizations.

Recommendations

Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations intend to allow individuals and groups to recognize IT security concerns and to respond accordingly.[3] Moreover, in cyber security situational awareness considers being a threat operation, such as threat activity and vulnerability in context that it can actively defend data, information, knowledge and wisdom from compromise.

Contemplating the slow progression toward cyber security, it is in fact important that the Macedonian authorities would take into action approaches moving forward to situational awareness. For instance, drafting a national strategic approach to build on the principles like the ones underlying Finland's cyber security strategy, such as: to improve comprehensive cyber security situation awareness of different actors; national and international cooperation in preparedness.[15] Where in the end such approach

could furnish them with real-time, shared and analysed information about vulnerabilities, disturbances and their effects, with agility and situational awareness. Secondly, in the field of IT and cyber security education and training it is in fact crucial to use the Estonian approach forming a national provider of training and awareness-raising, known as Information Technology Foundation for Education (HITSA).[42] The last contribution is by building sustainable cyber security culture including: human resource development; organizational development; institutional and legal framework development; educational efforts and investments; and continuous training.[43]

In this light we might conclude from the earlier analysis that the existing awareness campaigns in Macedonia are broadly in-line to target groups such: children, parents and teachers; as well as institutional awareness, on one hand. On the other hand, it dispenses campaigns throughout the publicly available website, posters, videos, and caravans. In addition, awareness-raising format is by designing standards, training and education. Speaking of education, presently in the country there is only one bachelor program available in the private New Man's Business Accelerator concentrating on Computer Networks and Cyber Security,[44] where on the national level there is a Master of Science and Doctor of Philosophy curriculum offered by the Faculty of Computer Networks Security from the University of Information Science and Technology "St. Paul The Apostle."[45] Finally, it was recently announced that the government will develop new defence studies university to include, among others, cyber security programs.

Although awareness is in the draft strategy, still it is important to emphasize that awareness must reflect the vision, the culture and the history of a nation by consideration of the global dimension and the education by highlighting the weakest link in cyber security as reference to the end-user. If considered, this could introduce and develop the cyber security culture, followed by awareness, education, training and campaigns. Thus, development of interdisciplinary training will be a real added value to awareness and permitting the nation to deal with a large range of cyber security threats. Followed by the continuous training which should not be omitted in order to prepare professionals to face the evolving and dynamic context of technology and threats.[43] In this fashion, it also will be fair to see campaigns' materials available not only in Macedonian and Albanian language, but also in English, and officially recognized minority languages: Turkish, Serbian, Romani, Bosnian and Vlach.

Last but not least, it is well known that the Balkan region has no fewer targets than elsewhere vulnerable to cyber attacks, especially when it comes to large-scale attacks. Yet, there are countries that are quickly progressing, while others are slowly moving forward. Still, the conclusion is that if we think towards situational awareness and awareness-raising, we can consider the establishment of a national provider of training and awareness-raising; such are tendencies in the Estonian and Finish approaches.

Figure 4 depicts establishment of IT security awareness campaigns for government and private organizations by implying different levels, such as: beginning, intermediate and advanced.

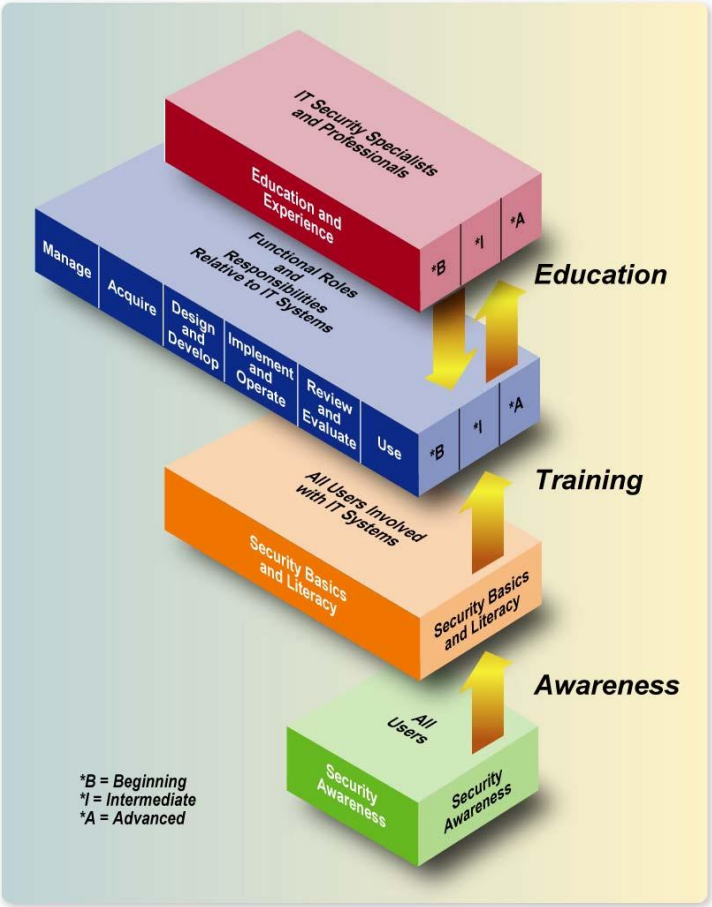

Figure 4: The IT Security Learning Continuum.[3]

Conclusion

Key contribution of this article aims to give an analysis of Macedonian IT and cyber security awareness campaigns brought by government, NGOs, and schools. It includes analyses of the three NGO and government campaigns organised so far, with similar target groups and various formats, and one study carried out in high schools. Meanwhile, government agencies are on the run to setup a national corresponding

body to work as an incident response team by announcements and basic awareness. A related requirement is to develop a national cyber security strategy which will deal with standards, training, education and campaigns. The NGO approach was through campaigns to focus on the youth, parents and teachers in the way of tips, guides on websites, caravans, posters, interactive videos, etc. The study analysed those campaigns and provided recommendations for raising further the level on IT and cyber security awareness in Macedonia in the light of continuous education, materials available in officially recognized minority languages, as well as by using as example the methods in Finland's cyber security strategy and the Estonian approach.

Finally, we believe that, if applied, the suggestions will introduce and raise the awareness at national level through extending the cyber security culture and situational awareness. This author will continue to follow the progress in his future publications.

Notes:

1 OECD, *OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security*, OECD Council, 2002.

2 European Network and Information Security Agency (ENISA), *The New Users' Guide: How to Raise Information Security Awareness*, November 29, 2010.

3 Mark Wilson and Joan Hash, *Building an Information Technology Security Awareness and Training Program, Computer Security*, NIST Special Publication 800-50, October 2003.

4 *OSCE Guide on Non-military confidence-building Measures (CBMs)*, http://www.osce.org/cpc/91082, accessed October 23, 2015.

5 State Statistical Office, "Information Society," http://www.stat.gov.mk/OblastOpsto_en.aspx?id=27, accessed December 29, 2015.

6 Ministry of Information Society of Macedonia, "Developed Information Society," http://www.mioa.gov.mk/files/pdf/Broshura_MIO_design_FINALNO.pdf, accessed June 15, 2015.

7 H. Raghav Rao and Shambhu Upadhyaya. *Information Assurance, Security and Privacy Services*, first edition (UK: Emerald Group Publishing Limited, 2009).

8 Ministry of Information Society and Administration of Macedonia, "Establishment of a National Body for Dealing with Computer Incidents (National CIRT)," August 8, 2012, http://www.mioa.gov.mk/?q=node/3198.

9 European Commission, "Commission Staff Working Document: The Former Yugoslav Republic of Macedonia Report 2015," Brussels, 10.11.2015, p.40, http://ec.europa.eu/enlargement/pdf/key_documents/2015/20151110_report_the_former_yugoslav_republic_of_macedonia.pdf.

10 ENISA, "CSIRTs by Country - Interactive Map," http://www.enisa.europa.eu/activities/cert/background/inv/certs-by-country-interactive-map, accessed on 21 April 2015.

[11] Ministry of Information Society and Administration of Macedonia, "Establishment of a National Body for Dealing with Computer Incidents (National CIRT)," www.mioa.gov.mk/?q=node/3198.

[12] UNDP, "International Expert for Preparation of an Assessment Study for the Requirements for Preparation of a National Cyber Security Strategy," 5 March 2014, http://jobs.undp.org/cj_view_job.cfm?cur_job_id=43974, accessed August 12, 2015.

[13] Republic of Macedonia, Ministry of Foreign Affairs, http://mfa.gov.mk/index.php/mk/, accessed August 17, 2015.

[14] Besnik Limaj, "Enhancing Cyber Security: The Challenges in FYROM, Kosovo and Moldova," January 5, 2015, http://www.observatoire-fic.com/contribution-enhancing-cyber-security-the-challenges-in-fyrom-kosovo-and-moldova/.

[15] Secretariat of the Security Committee, *Finland's Cyber Security Strategy*, January 2013.

[16] ENISA, "ENISA Threat Landscape 2014: Overview of Current and Emerging Cyber Threats," December 2014.

[17] Predrag Tasevski, *Interactive Cyber Security Awareness Program* (Germany: Lambert Academic Publishing, 2012).

[18] Adel Abusara, "A Comprehensive Cyber Awareness Campaign – A 'Prequel' to Strong and Lasting Cybersecurity PPP in Serbia," DCAF Young Faces 2014 – Cybersecurity Winter School for the Western Balkans, 2014.

[19] Surf Safely, IFS-EMMAUS, http://sigurnodijete.ba/en/, accessed August 13, 2015.

[20] CyberCrime.BG, http://www.cybercrime.bg/bg, accessed August 13, 2015.

[21] Kids Online, Bulgarian Safer Internet Node, http://www.safenet.bg/index.php?id=1389, accessed August 13, 2015.

[22] Bulgarian Hotline for Fighting Illegal and Harmful Content in Internet, http://web112.net/en/NewSignalEN.aspx, accessed August 13, 2015.

[23] Cyberalbania, http://cyberalbania.al/, accessed August 13, 2015.

[24] Centar za sigurniji internet, http://www.sigurnijiinternet.hr/, accessed August 13, 2015.

[25] Children's Rights on the Internet – Safe and Protected, http://crisp.org.mk/, accessed July 27, 2015.

[26] Surf Safe, http://surfajbezbedno.mk/#dom, accessed July 27, 2015.

[27] Privacy, http://privatnost.mk/en/, accessed December 27, 2015.

[28] Metamorphosis, "About," http://metamorphosis.org.mk/en/about/, accessed August 12, 2015.

[29] Metamorphosis, "Children's Rights on the Internet – Safe and Protected," http://metamorphosis.org.mk/en/proekti_arhiva/childrens-rights-on-the-internet-safe-and-protected/, accessed August 12, 2015.

[30] DPDP, http://dzlp.mk/mk/cpp, accessed December 28, 2015.

[31] Sitemeter.com, "Bezbedno na internet," Site Summary, http://www.sitemeter.com/?a=stats&s=s45crisp"s=s45crisp, accessed August 12, 2015.

[32] CRISP, "Day of the Safe Internet – To Create a Better Internet Together" (in Macedonian), http://bezbednonainternet.org.mk/content/view/335/1/lang,mk, accessed August 8, 2015.

[33] Safer Internet Day, http://www.saferinternetday.org/web/guest/home, accessed August 13, 2015.

[34] MIO, "Promotion campaign for safety of children and youth of the Internet 'Surf Safe'," March 10, 2013 (in Macedonian), http://www.mio.gov.mk/?q=book/export/html/3363, accessed August 12, 2015.

[35] FINKI, http://www.finki.ukim.mk/en/home, accessed August 12, 2015.

[36] AEK, http://www.aek.mk/en/, accessed August 12, 2015.

[37] TACSO, http://tacso.org/project-org/Macedonia/?id=21, accessed August 12, 2015.

[38] Predrag Tasevski, "I can hack your FB, can you catch me...," May 26, 2013, http://predragtasevski.com/posts/2013/05/i-can-hack-your-fb-can-you-catch-me/, accessed August 12, 2015.

[39] Privatnost.mk, http://privatnost.mk/en/summary/, accessed December 27, 2015.

[40] e-Society.mk, http://www.e-society.org.mk/. accessed December 27, 2015.

[41] "Research and Analysis of Responses to the Questionnaire for Pupils of Secondary Schools of the City of Skopje – Project Class for Privacy" (in Macedonian), Metamorphosis and DPDP, January 2015, http://dzlp.mk/sites/default/files/u972/Istrazuvanje.pdf.

[42] Ministry of Economic Affairs and Communication, "Estonia, Cyber Security Strategy 2014-2017" (2014).

[43] Stein Schjølberg and Solange Ghernaouti-Hélie, *A Global Protocol on Cybersecurity and Cybercrime: An initiative for peace and security in cyberspace*, Cybercrimedata 2009, (Oslo: E-dit, 2009).

[44] New Man's Business Accelerator, "Computer Networks and Cybersecurity," http://newmansba.com/computer-networks-and-cybersecurity/, accessed August 17, 2015.

[45] "Faculty of Computer Networks Security," University of Information Science & Technology "St. Paul The Apostle," Ohrid, http://uist.edu.mk/Academics/CNS_p, accessed December 27, 2015.

About the Author

Predrag TASEVSKI holds a MSc degree in Engineering in the field of cybersecurity from Estonia, and a Post-Master in Communication and Security from elite school in France. Currently he is a PhD Candidate at TTU - Estonia. His research interests are in the field of cybersecurity, cyber defence, security awareness, risk assessment, risk management, cyber risk, cyber insurance, cybersecurity awareness, socio-technical aspects, data science and hacktivism. Predrag is the author of two paperback books and has published in several international journals and conferences. He is also a Microsoft Certified Trainer and a Lead/External Auditor for ISMS. At present, he is a founder of CyberSecurity.mk – Research and Development company based in Macedonia. *E-mail:* pece@cybersecurity.mk.