Alexander Balthasar, Blaž Golob, Hendrik Hansen, Balázs Kőnig,
Robert Müller-Török, Alexander Prosser

Central and Eastern European e|Dem and e|Gov Days 2015

Time for a European Internet?

Conference Proceedings

© Austrian Computer Society 2015

© Österreichische Computer Gesellschaft
Komitee für Öffentlichkeitsarbeit
www.ocg.at

Druck: Druckerei Riegelnik
1080 Wien, Piaristengasse 19

ISBN 978-2-85403-308-0

E-SAFETY, PRIVACY AND INFORMATION SECURITY: REQUIREMENTS IN PUBLIC ADMINISTRATION

Csaba Krasznay[1], Gábor Törley[2]

Abstract

According to the results of a representative survey by ESET Hungary Ltd. and statistics by Eurostat, more than one million users in Hungary visit infected webpages despite of warnings of their antivirus program and almost every second an individual caught a virus or other computer infection (worm, Trojan horse, etc.). These data are similar to those in Slovenia, in Croatia, in Slovakia and in Bulgaria. This may be caused by low levels of security awareness and independent from any typical statistical distribution (e.g. age, sex, geographic location, etc.). Therefore this security unpreparedness appears in all work places, including Public Administration.

Those who work in Public Administration manage other people's personal data, but how could they manage them securely if they cannot be vigilant with their own personal data? We believe that security awareness is a way of thinking which is teachable and learnable, and should be developed as a basic knowledge in primary and secondary education and later upgraded as a special knowledge at public administration schools.

We discuss three topics: (1) a comparison of what pupils are taught on e-safety, privacy and information security in Hungary and England to understand the level of basic knowledge; (2) an international overview about governmental requirements from an average employee in Public Administration on e-safety, privacy and information security to understand what special knowledge is required on this field; (3) some best practices how we can give the special security knowledge for these people at university level in order to meet the requirements of Public Administration. We use U.S. and U.K. examples, because these countries have the most mature cybersecurity system and best-described use cases in all areas examined by this study. We also examine EU's special requirements because Hungary, as a member state should follow these rules and guidances.

1. Introduction

Recent representative surveys in Europe and in Hungary raise questions about the level of information security awareness of an average user. According to the results of a representative survey in 2011 by ESET Hungary Ltd., more than 1 million Hungarian Internet users open dangerous webpages, despite of warnings from their antivirus system. Moreover, 10% of Hungarian Internet users switch off intentionally their antivirus software in response.

This is mostly typical in the age group 18-29, that is 17% of the Hungarian Internet users. Older people (age group 50-69) are the most careful users. 15% of men and only 6% of women open a file which is marked as virus infected. [1]

[1] National University of Public Service, Faculty of Public Administration, H-1118 Budapest Ménesi út 5., krasznay.csaba@uni-nke.hu, http://en.uni-nke.hu

[2] National University of Public Service, Faculty of Public Administration, H-1118 Budapest Ménesi út 5., torleyg@office.uni-nke.hu, http://en.uni-nke.hu

This kind of attitude leads to a negative conclusion. According to the Symantec Intelligence Report [15], in March 2011 Hungary was the 3rd on the "world ranking list of spam", meaning 85.8% of the country's e-mails were spam. Eurostat's results show that 46% of computers connected to the Internet are infected by viruses. [5] This means almost every second computer is affected. Slovenia, Croatia, Bulgaria and Slovakia had similar results.

Country	*Caught a virus or other computer infection (worm, Trojan horse, etc.)*
Croatia	33%
Slovenia	37%
Hungary	46%
Slovakia	47%
Bulgaria	58%

Table. 1. Caught a virus or other computer infection (worm, Trojan horse, etc.) per country

It is especially disquieting that security awareness amongst age group 18-29 is so low because this group includes those young men and women who just finished their secondary education.

2. Information security and data protection in the Hungarian curriculum framework

The Hungarian curriculum framework is regulated by the Ministry of National Resources. [10] Curriculum framework defines those knowledge elements that a pupil should know after finishing a grade and specifies the minimum lesson hours[3] per week for each subject and grade. The table below shows the distribution of lesson hours for the *Informatics* subject.[4]

	Grade 5	*Grade 6*	*Grade 7*	*Grade 8*	*Grade 9*	*Grade 10*	*Grade 11*	*Grade 12*	*Sum.*	*% of all lessons*
Informatics	0	1	1	1	1	1	0	0	180	1,93%
Amount of free lesson hours	2	3	3	3	4	4	6	8	1188	12,74%
All lesson hours	28	28	31	31	35	36	35	35	9324	100%

Table. 2. Distribution of lesson hours for the Informatics subject

In Hungary schools can add more lesson hours to the subject's minimum lesson hours from the free lesson hours. According to the surveys of Association of Hungarian Informatics Teacher and Ministry of National Resources, schools generally don't use or use only a few of these free hours to increase the informatics' lesson hours (see Fig. 1.). [14]

[3] One lesson hour = 45 minutes

[4] Last two columns are not part of the official table, those based on our counting

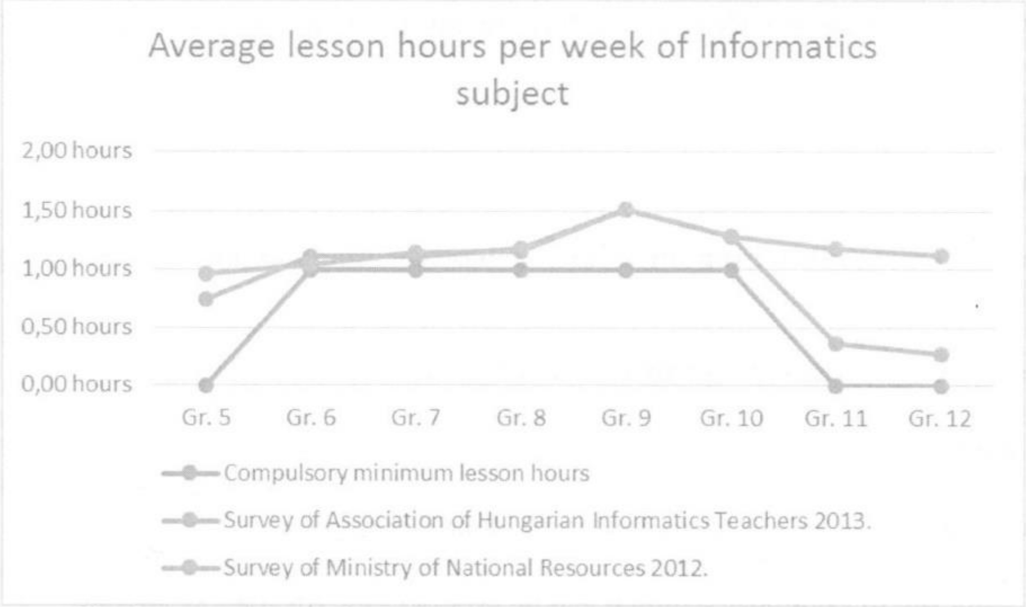

Fig. 1. Average lesson hours per week of Informatics subject in Hungary

In Hungary, the major textbook publishers made sample curriculums based on the curriculum framework for their textbooks. The table above shows, how many lesson hours are used in grades 5-12 for information security (IS) and data protection (DP).

	Lesson hours		
Publisher[5]	*IS and DP*	*Informatics*[6]	*% of inf. lesson hours*
AK	5	212	2%
Mozaik	6	250	2%
KPSZT	7	180	4%
JOS	12	252	5%
NTK	7	180	4%

Table. 3. Lesson hours for IS and DP per publisher

We think that there might be a connection between the very few lesson hours and the result of ESET Hungary Ltd.'s survey. Few lesson hours and few attention can lead to low security awareness. To prove this statement, further research is needed which is not covered in this paper, but comparing the results of [3] and [5], usually those countries which cover all the topics of online safety issues, had better results in the Eurostat's survey. We assume that more lesson hours are needed to cover more topics.

[5] Apáczai Publisher (AK), Mozaik Publisher (Mozaik), Catholic Pedagogy Organization and Training Institute (KPSZT), Knowledge of Generations Textbook Publisher (NTK), Jedlik Education Studio (JOS)

[6] KPSZT and NTK used the compulsory minimum lesson hours, the others used more.

These topics should be covered according to the Hungarian curriculum framework:

Grade 5-6.

- Using IT tools
    - log in/log off to/from the school network, getting to know and observing rules of the school network
    - getting to know to use an antivirus software
- Information society
    - concepts of information security and data protection
    - getting to know ways which can be applied towards data protection
    - getting to know the rules of ethical use of IT tools

Grade 7-8.

- Info communication
    - distinguish between data that can be public and that should be protected
- Information society
    - concepts of information security and data protection
    - risks and consequences of misused data
    - getting to know trustworthy information sources
    - ability to evaluate the trustworthiness of information

Grade 9-10.

- Using IT tools
    - getting to know the hardware and software ways of data protection
- Information society
    - concepts of data protection
    - ability to evaluate information sources

3. Information security and data protection in English[7] core curriculum

From September 1st 2014, a new core curriculum became effective in England. Its philosophy differs from the Hungarian curriculum, because it declares only goals and topics and it doesn't prescribe how many minimum lesson hours should be used for each topic in each grade. The regulation gives schools the right to make a decision on this. An important principle: schools should spend enough time in order to have a widespread, balanced and eligible curriculum. [12]

The grades mentioned in the Hungarian curriculum framework (5-12) correspond with Key Stage 3 (11-14 years old pupils) and 4 (14-16 years old pupils) in the English curriculum.

English curriculum defines a general goal: pupils should be responsible, competent and confident users of information and communication techniques (ICT).

Pupils should reach these goals in Information security and data protection at each key stages: [9]

Key stage 3

- pupils should be taught to understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy; recognize inappropriate content, contact and conduct and know how to report any concerns

Key stage 4

- pupils should be taught to understand how changes in technology affect safety, including new ways to protect their online privacy and identity, and how to identify and report a range of concerns

Goals in the English curriculum focus more on practical methods and understanding than knowledge like in the Hungarian curriculum framework. This seems to be a philosophical difference between the two countries' curriculum.

We asked 18 secondary school teachers from England to complete a survey on how many lesson hours they use in a year for Information security and data protection.

According to our results, these teachers teach on average 13.39 lesson hours in Key Stage 3 and 4 (Year 7-11). It is approx. two times more than in Hungary. The diagram below shows (see Fig. 2.) that the majority of lesson hours are used in Year 7 and 8. This is a good method because pupils meet mostly with the risks of the Internet at this age and with learning important principles in greater amount of lesson hours can help them to grow their security awareness.

[7] We will discuss only the core curriculum of *England*, not of the United Kingdom (UK), because countries in the UK have the right to create their own curriculum and the English one has been reformed recently.

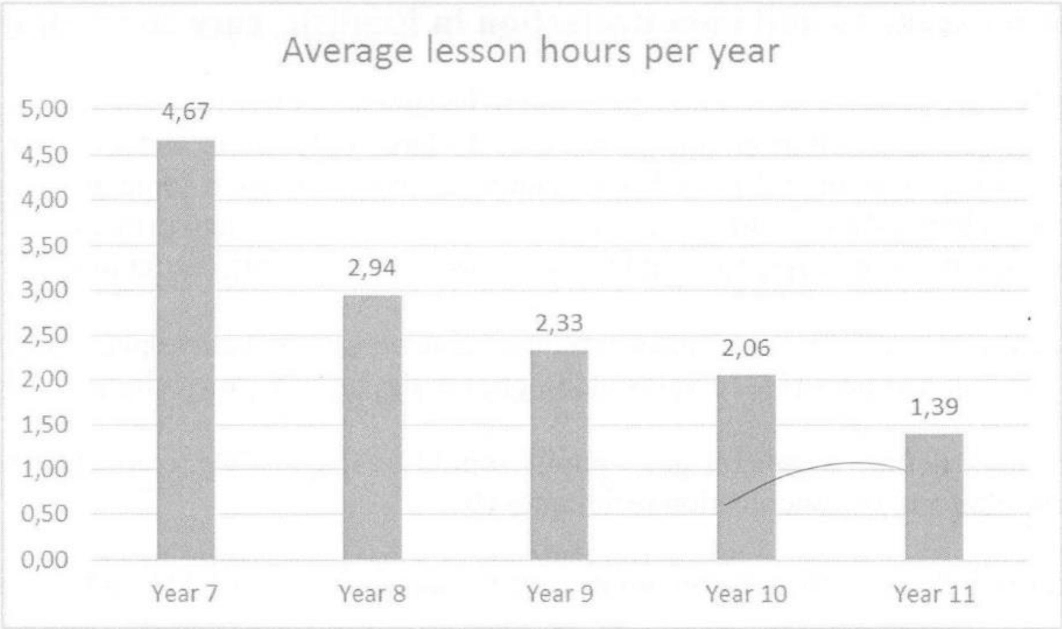

Fig. 2. Average lesson hours per year used for IS and DP

From the distribution of lesson hours (see Fig. 3.) we can see that half of the teachers use 15 hours or more for teaching information security and data protection in Year 7-11.

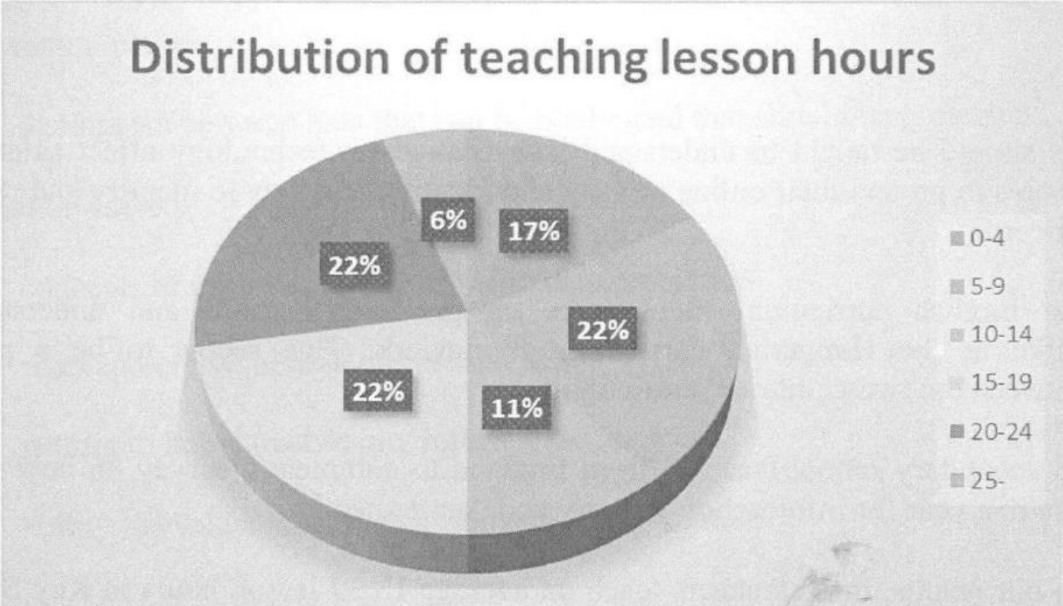

Fig. 3. Distribution of teaching lesson hours for IS and DP in Year 7-11.

According to [3], topics like cyberbullying, safe use of mobile phones and contact with strangers are not included in Hungarian education programmes. English teachers in our survey generally covered all the important topics of IS and DP (Online safe behavior, Privacy issues, Cyberbullying, Downloading issues, Safe use of mobile phones, Contact with strangers, Safe use of social networks, Use of antivirus softwares, Password policy).

4. Cybersecurity at university level

In the previous sections we examined how basic security awareness would be gained at public education. The following sections discuss how special security knowledge could be built at university level, because cybersecurity is one of the most terrifying challenges in a modern society and employees of public administration should be ready to understand this challenge.

No one can measure the real impact of an organized cyberattack against a country. Economies as well as governments are heavily rely on interconnected information systems. In practice successful cyberattacks usually contains some human intelligence (so called HUMINT) elements, therefore higher information security awareness can reduce the attack surface, or at least this is a common understanding between security experts. Different traditional security related topics are still part of the education of public servants, so it seems feasible to make a chance on the involvement of cybersecurity into regular and irregular education activities dedicated to the public sector.

As previous sections described, university freshmen in public administration universities usually have some basic security knowledge originated from elementary and secondary schools all over Europe. In one hand this covers only the basics on the other hand this knowledge varies from country to country. Furthermore we shouldn't forget those public servants who are working in public service for years or decades without these security basics. So if a country wants to improve cybersecurity readiness inside its own system and wants to extend awareness in European level, some widely implemented trainings are necessary.

Some highly exposed countries have these kind of trainings for years. As in many cybersecurity fields, United States is the pioneer on nationwide awareness programs, therefore it is a good starting point to understand its cybersecurity education system that might have some positive effects on public servants' security awareness level.

U.S. National Cyber Security Awareness Month was launched by the National Cyber Security Alliance and the U. S. Department of Homeland Security in 2004 and was developed for thematic weeks in 2012 based on feedback. [6] Among others this improvement (cf. better identification of cyberattack signs by employees) may led a significant jump in reported incidents by federal agencies to US-CERT in 2013, based on United States Government Accountability Office's analysis. [17]

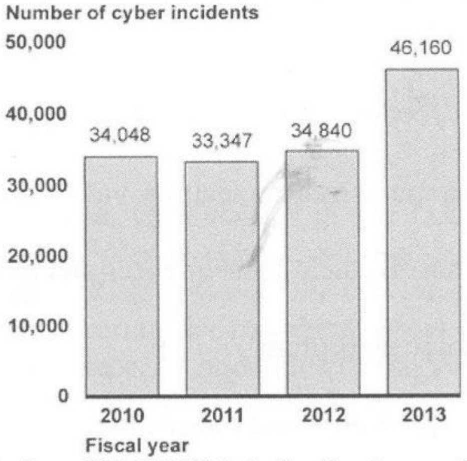

Fig. 4. GAO analysis on US-CERT data for fiscal years 2010-2013. Source: [17]

The Stop.Think.Connect. campaign is the essential part of the National Cyber Security Awareness Campaign. [13] Its organizer is the Department of Homeland Security. It has special resources for both federal, state and local government organizations. For federal government actors it offers some general and specific programs. These are the followings (excerpt):

- DHS and the National Security Agency (NSA) co-sponsor the National Centers of Academic Excellence in Information Assurance Education (CAE/IA), CAE-Research (CAE-R), and the two-year (CAE2Y) programs, which promote higher education in cybersecurity and produce growing numbers of IA workers.

- DHS and the National Science Foundation offer the Scholarship for Service Program (SFS) to outstanding undergraduate, graduate and doctoral students in exchange for government service at a Federal agency. SFS is building a strong pipeline of skilled employees to fill critical IA positions.

- The Federal Virtual Training Environment (FedVTE) provides online access to more than 800 hours of classroom training and 75 hands-on labs to more than 125,000 federal employees.

- The Federal Cybersecurity Training Exercise (FedCTE) provides interactive events that bring federal participants together to share cybersecurity best practices in a secure, simulated environment. [2]

The U.S. Government also introduced some supporting materials for agencies to create useful and efficient awareness training. National Institute of Standards and Technology's Computer Security Division is responsible to create such guidance. Its Special Publication 800-16 is about "Information Technology Security Training Requirements: A Role- and Performance-Based Model" and Special Publication 800-50 is about "Building an Information Technology Security Awareness and Training Program". These two materials form the framework of awareness training for federal employees.

NIST Special Publication 800-16 Revision 1 (3rd Draft) has some cybersecurity specialties. "The Cybersecurity Essentials level on the Cybersecurity Learning Continuum is the transition between Security Awareness and Role-Based training. (…) Cybersecurity Essentials refers to an individual's familiarity with – and ability to apply – a core knowledge set which is needed to protect electronic information and systems. The Cybersecurity Essentials level key terms, essential concepts and principles include an understanding of:

- Technical underpinnings of cybersecurity and its taxonomy, terminology and challenges;

- Common information and computer system security vulnerabilities;

- Common cyberattack mechanisms, their consequences and motivation for use;

- Different types of cryptographic algorithms;

- Intrusion, types of intruders, techniques and motivation;

- Firewalls and other means of intrusion prevention;

- Vulnerabilities unique to virtual computing environments;

- Social engineering and its implications to cybersecurity; and

- Fundamental security design principles and their role in limiting point of vulnerability." [16]

According to Ponemon Institute's "2014 Best Schools for Cybersecurity" survey, University of Texas, San Antonio has the most comprehensive cybersecurity offering for students and naturally is the part of the National Centers of Academic Excellence in Information Assurance Education. [11] This university also has a BA program in Public Administration. Direct cybersecurity classes for public administration students are very rare so it is very interesting how the so called "best" cybersecurity knowledge connects to a public administration BA program and as a use case how it relates to the federal requirements defined in NIST SP 800-16!

"Principles of Information Systems for Management" is a prescribed course for students. Instructors usually use Essentials of Management Information Systems (Eleventh Edition) by Laudon and Laudon as textbook. Its Chapter 8 "Securing Information Systems" deals with the questions of cybersecurity with some useful cases, e.g. "Stuxnet and Cyberwarfare" and "Cyberespionage: The Chinese Threat". It also contains a chapter in "Ethical and Social Issues in Information Systems" with cases about net neutrality and privacy. [8]

"Introduction to Cyber Security" is a good example for a full semester course dedicated for security awareness for Bachelor of Business Administration. Although its name reflects to cybersecurity, it is a well-designed lab activity for average users about ordinary security practice. [18] Convergence of public administration studies and cybersecurity awareness is clear but direct appearance of federal requirements in these subjects is not evident.

This maturity level is not yet appeared in the European Union, although EU's Digital Agenda for Europe clearly states that this is a high priority topic both in Europe and member states. Therefore EU member states shall work together to maintain a good cybersecurity ecosystem. Some common guidance can help in reaching this goal. European Union Agency for Network and Information Security (ENISA) is the main source of such guidance.

ENISA published its "Roadmap for NIS education programmes in Europe" in October 2014. [1] This study also contains an analysis about nationwide European information security initiatives, including some relevant university courses. Security related courses in different European universities are also linked in this study. According to this analysis future employees of the public sector are not targeted with specific courses, however the United Kingdom is mentioned as a very good example.

Cybersecurity awareness spreading is very similar in the U.K. and in the United States. In the United Kingdom "the National Archives is responsible for delivering a training and engagement programme for Senior Information Risk Owners (SIRO), Information Asset Owners (IAO), non-executive directors, board and audit committee members across the public sector. The programme is sponsored by the Office of Cyber Security and Information Assurance in the Cabinet Office and forms part of the National Cyber Security Programme." [7]

It seems that at EU level there isn't any specific programme for public servants on cybersecurity. Although the European Committee for Standardization (CEN) in its workshop agreement CWA 16624-1 "e-Competence Framework for ICT Users - Part 1: Framework Content" has some proposal how security awareness should appear in an ordinary ICT course. According to this document an average user should be aware with document and content security in word processing and spreadsheets, security questions of web browsing and secure communication on the internet. But this doesn't mention the challenges of cybersecurity. [4]

5. Summary

Because of the special cybersecurity risks of public sector we propose a pan-European cybersecurity education programme for public servants at university level. This education programme should be built on basic ICT security skills coming from the secondary schools or from own experience and should focus on the handling of special challenges. Although many elements are still available for such courses, a targeted best practice is not yet presented by ENISA.

In Hungary we tried to start a special program for public servants at the National University of Public Administration (NUPS) in Budapest. We tried to formulate a curriculum that contains a deep awareness programme for B.A. and M.A. students of Public Administration. This curriculum deals with both security and privacy questions. NUPS has a special status in Hungary, it also runs the central law enforcement and military courses that is why (cyber)security can be emphasized in its bachelor and master programme.

To reach this goal a unified approach would be needed, but current European guidelines are not mature enough to be built on. At NUPS we teach both data protection and information security, therefore students would understand and apply this unified approach. B.A. students has two mandatory classes about Information Systems in Public Administration with heavy information security inclusion. These classes also contain laboratory practices about security issues. They can elect many other classes in this topic.

The new curriculum was introduced at the fall of 2014 in the B.A. of Public Administration, therefore we can provide more data later on, in separate studies. Our first experience shows the lack of basic awareness. Although there isn't much experience with this programme it is evident that the Hungarian government support this direction. In its National Infocommunication Strategy 2014-2020 cybersecurity is one of the main pillar. In the following years we at NUPS will shape this programme, work together with responsible governmental institutes and give more information for the European academic community about our results.

6. References

[1] BERENDT B.; DE PAOLI S.; LAING C.; FISCHER-HÜBNER S.; CATALUI D.; TIRTEA R., Roadmap for NIS education programmes in Europe, European Union Agency for Network and Information Security, Athens 2014

[2] DEPARTMENT OF HOMELAND SECURITY, Federal Government Offerings, Products and Services, [1] ESET Hungary Ltd.'s survey - http://www.eset.hu/hirek/kivancsisagunk_fertoz ?back=/hirarchivum%3Fpage%3D9 in Hungarian – Downloaded October 28th 2014.

[3] Eurodyce (2011): Key Data on Learning and Innovation through ICT at School in Europe 2011

[4] EUROPEAN COMMITTEE FOR STANDARDIZATION, CWA 16624-1, e-Competence Framework for ICT Users - Part 1: Framework Content, Brussels 2013

[5] Eurostat (2011): Nearly one third of internet users in the EU27 caught a computer virus, In: Eurostat Newsrelease 21/2011

[6] History of NCSAM – http://www.staysafeonline.org/ncsam/about/history-of-ncsam – Downloaded: January 15th 2015

[7] Information Assurance and Cyber Security training – http://www.nationalarchives.gov.uk /information-management/training/information-assurance-training/ – Downloaded: January 15th 2015

[8] LANDON, K. C.; LANDON, J., Essentials of MIS, 11/E, Prentice Hall, New York 2015

[9] National curriculum in England: computing programmes of study – https://www.gov.uk/ government /publications/national-curriculum-in-england-computing-programmes-of-study – Downloaded: January 15th 2015

[10] Nr. 51/2012. (XII. 21.) decree of Ministry of National Resources – in Hungarian

[11] PONEMON INSTITUTE LLC, 2014 Best Schools for Cybersecurity, North Traverse City 2014

[12] Recommended Annual Instruction Time in Full-time Compulsory Education in Europe 2013/14 In. Eurydice – Facts and Figures – http://eacea.ec.europa.eu/education/eurydice /documents/facts_and_figures/Instruction_Time_2013_14.pdf – Downloaded: November 11th 2014.

[13] Stop.Think.Connect. – http://www.dhs.gov/stopthinkconnect – Downloaded: January 15th 2015

[14] Surveys of Association of Hungarian Informatics Teacher and Ministry of National Resources – http://isze.hu/download/Informatika_felmeres_honlapra.pdf – in Hungarian – Downloaded: January 15th 2015.

[15] Symantec.cloud MessageLabs Intelligence: March 2011 Intelligence Report – http://ambientesicurezza.ilsole24ore.com/whitepaper_library/symantec_intelligence_rpt_mar_ 2011.pdf – Downloaded: November 4th 2014.

[16] TOTH P; KLEIN P., NIST Special Publication 800-16 Revision 1 (3rd Draft), A Role-Based Model for Federal Information Technology/Cybersecurity Training, National Institute of Standards and Technology, Gaithersburg (2014)

[17] UNITED STATES GOVERNMENT ACCOUNTABILITY OFFICE, Agencies Need to Improve Cyber Incident Response Practices, Washington 2014 Washington, 2014

[18] YOUNG, D., IS1503 Introduction to Cyber Security Syllabus University of Texas (2014)