INDIVIDUAL AWARENESS OF CYBER-SECURITY VULNERABILITY – CITIZEN AND PUBLIC SERVANT

Krisztina Győrffy[1], Ferenc Leitold[2] and Anthony Arrott[3]

Abstract
Cyber-security is not concerned so much with average or median vulnerability in an organization. Rather more important is identifying the weakest links. Individual user susceptibility and user behaviour risk assessment are key to measuring the effectiveness of cyber-security awareness programs and policies. Increasingly, it has been demonstrated that managing individual user susceptibility is as critical to organization well-being as maintaining patched IT infrastructure or responding to specific immediate cyber-threat alerts.

Despite IT systems audits, human factor studies, training courses, user policies, and user documentation, managing user cyber-security awareness remains one of the weakest links in protecting organizations from cyber-threats. Most employees are not aware of the cyber-threats they are most likely to encounter while performing their work. They are susceptible to malicious manipulation (social engineering threats) and they tend not to follow standard procedures (either through ignorance or in attempting to circumvent security procedures to achieve more productivity). Typically, employees only recognize the importance of cyber-security policies and practices after an incident has happened to themselves.

With the increasing availability and utility of IT network traffic analysis tools and active user behaviour probes (e.g., fake-phishing), employees can be given direct and individual feedback to increase their cyber-security awareness and improve their cyber-security practices. Beyond an organization's employees, the same holds for a country's citizens, or a government's public servants. At their best, these user behaviour monitoring tools can be used in an open and transparent way to increase awareness of individual vulnerability before actual incidents occur.

In addition to presenting results from the application of user behaviour monitoring tools to cyber-security, this paper examines the efficacy of the privacy protection safeguards that they incorporate. These results are applied to public sector approaches to: (a) public awareness of citizen cyber-health; (b) securing online pubic services; and (c) public servant awareness of their own vulnerability to cyber-threats.

Key words: *cybersecurity user behaviour, cyber-security user awareness, user behaviour monitoring tools, IT network traffic analysis.*

1. Introduction

At some level, all software processes are incompletely autonomous and require some degree of human decision-making to effectively perform useful work in information processing. Well-designed software user interfaces provide the human decision-maker with logic, context, and

[1] University of Pannonia, Secudit Ltd, kgyorffy@secudit.com
[2] Secudit Ltd., University of Dunaújváros, fleitold@secudit.com
[3] Secudit Ltd, aarrott@secudit.com

guidance which make the necessary human decisions easier and more reliably successful. However, residual risk always remains that cannot be completely eliminated as a hazard in the human decision-making process.

We can associate the best that software support of human decision-making can provide with full facilitation of what may be referred to as first-order learning about the software process by the user. Similarly, we can associate the concept of second-order learning as support for the user's judgement that is inherently beyond what the autonomous software application can provide [1].

When applied to natural hazards, such as circumstantial disruptions of software processes or accidents and mistakes of judgement by users, the second-order learning required to mitigate risk can be achieved using well-established concepts and techniques of risk communication and risk education [2]. However, when the hazards involve malicious intent, the entire first-order learning support system is susceptible to wholesale subversion. Malicious actor knowledge of the guileless software user interfaces and the predictable behaviors of even well-trained users give rise to vulnerabilities at the software user interface. Malicious exploitation of these vulnerabilities are referred to as malicious social engineering attacks [3,4] Consequently, the vulnerability of software users to social engineering attacks requires additional considerations for effective risk communication and risk education [5].

Effective mitigation of user susceptibility to social engineering requires active engagement of the users themselves in their own cyber-defense. Strong motivators for user responsibility and competence in cybersecurity include:

- business-context phishing emails remain the most difficult for users to recognize.
- top emotional motivators: curiosity, fear, urgency.
- susceptibility to phishing email drops almost 20% after just one failed simulation.
- reporting rates significantly outweigh susceptibility rates when simple reporting is deployed to more than 80% of a company's population, even in the first year
- active reporting of phishing email threats can reduce the standard time for detection of a breach to 1.2 hours on average—a significant improvement over the current industry average of 146 days. [6].

Government cybersecurity strategies and directives have emphasized the need for cybersecurity awareness and training for both public servants and private citizens [7,8,9]. Despite IT systems audits, human factor studies, training courses, user policies, and user documentation, managing user cyber-security awareness remains one of the weakest links in protecting organizations from cyber-threats. Most employees are not aware of the cyber-threats they are most likely to encounter while performing their work. They are susceptible to malicious manipulation (social engineering threats) and they tend not to follow standard procedures (either through ignorance or in attempting to circumvent security procedures to achieve more productivity). Typically, employees only recognize the importance of cyber-security policies and practices after an incident has happened to themselves.

With the increasing availability and utility of IT network traffic analysis tools and active user behaviour probes (e.g., fake-phishing), employees can be given direct and individual feedback to increase their cyber-security awareness and improve their cyber-security practices. Beyond an organization's employees, the same holds for a country's citizens, or a government's public servants. At their best, these user behaviour monitoring tools can be used in an open and transparent way to increase awareness of individual vulnerability before actual incidents occur.

2. Public awareness of citizen cyber-health

2.1 The correlations between government rules and human behaviour

In the Financial Times in the USA young directors can be concerned about tackling the problem of cyber security. [10]; while on the other side of the World in December 7, 2015, the European Parliament and the Luxembourg Presidency of the Council of the European Union (EU) reached an agreement on common rules to strengthen network and information security across the EU. It unveiled the proposed Network and Information Security Directive, the "NIS Directive". The "NIS Directive" constitutes the first and essential step for the development of an EU harmonized framework for cybersecurity. Earlier the United Kingdom (UK) Cyber Security Strategy was published in November 2011 and later in February 2012 the Government Regulation about the Hungary National Security Strategy was published in Hungary. [8]

It is real information, because it is proven that information systems used with the introduction of safety measures can reduce the number of cyber-incidents. However, with the ongoing increased introduction of rules available to mitigate identified risk you cannot reach an adequate level of reduction in cyber-attacks or loss of data. Junior directors, government's public servants or other country's citizens make important decisions without a depth and breadth of knowledge and experience across the area of information assurance. These mean real dangers and high degree of risk factors in the cyber-security landscape.

Due to the ability of the media and the research community to support a level of single focus, you can try to diagnose the cyber illness and measure the level of the awareness of cyber-security.
Nowadays the younger generation believe that cyber-security risk or the awareness of the cyber-security and the security cyber-regulations is new fashion in the world, and this issue solely is the problem of the security society. In this case security expects advice on the scale of the cyber threat, the risks that need to be considered by everyone at all times.
It is the great risk that the younger generation use the Internet and the different cyber-applications with self-confidence. By using the cyber without control the human obsession will take the dangerous way. In this event the cyber-device causes addiction and health damage for the citizens. Health damage is the cyber headache, dry eyes, vision deteriorations, tenosynovitis and musculoskeletal complaints or even psychiatric cases. In Hungary the Labour Code was released for the computer work in 2012 which says that the employer is obliged to organize the workflow so that continuous work hours for at least 10 minutes before the screen should be interrupted and actual work before the screen shall not exceed six hours daily.

2.2 Modern awareness security

The professional security societies such as Cyber-Security organisations in United States of America [13] [14] or the United Kingdom Cyber Essentials draw attention to the risks and publish topics of Cyber Security Controls.

The next table presents the topics of security instructions for the citizens or security experts by Cyber-Security institutes [15] such as Centre for Internet Security. [14]

Top 10 2013-A6-Sensitive Data Exposure

2013 Table of Contents

← A5-Security Misconfiguration | 2013 Top 10 List | A7-Missing Function Level Access Control →

Threat Agents	Attack Vectors	Security Weakness		Technical Impacts	Business Impacts
Application Specific	Exploitability DIFFICULT	Prevalence UNCOMMON	Detectability AVERAGE	Impact SEVERE	Application / Business Specific
Consider who can gain access to your sensitive data and any backups of that data. This includes the data at rest, in transit, and even in your customers' browsers. Include both external and internal threats.	Attackers typically don't break crypto directly. They break something else, such as steal keys, do man-in-the-middle attacks, or steal clear text data off the server, while in transit, or from the user's browser.	The most common flaw is simply not encrypting sensitive data. When crypto is employed, weak key generation and management, and weak algorithm usage is common, particularly weak password hashing techniques. Browser weaknesses are very common and easy to detect, but hard to exploit on a large scale. External attackers have difficulty detecting server side flaws due to limited access and they are also usually hard to exploit.		Failure frequently compromises all data that should have been protected. Typically, this information includes sensitive data such as health records, credentials, personal data, credit cards, etc.	Consider the business value of the lost data and impact to your reputation. What is your legal liability if this data is exposed? Also consider the damage to your reputation.

Am I Vulnerable To 'Sensitive Data Exposure'?

The first thing you have to determine is which data is sensitive enough to require extra protection. For example, passwords, credit card numbers, health records, and personal information should be protected. For all such data:

How Do I Prevent 'Sensitive Data Exposure'?

The full perils of unsafe cryptography, SSL usage, and data protection are well beyond the scope of the Top 10. That said, for all sensitive data, do all of the following, at a minimum:

Table 1: in 2013 table of controls, Top 10 Sensitive Data Exposure by The Open Web Application Security Project, not-for-profit charitable organization in the United States of America

However, the security experts or the citizens with behavior of modern awareness security know the top controls (Table 1 and Table 2) even if they don't follow the instructions, but analyze who is the person without awareness of cyber-security. On the base of the observation and of the information security research we can diagnose that the citizen without awareness of cyber-security is indeed insecure in the cyber-world. Such citizens can't securely use cyber applications and cyber devices. They are the citizens who are frightened by the notice on the screen and don't notice the cyber-incident or virus infection.

Top 5 CIS Controls

- CSC 1: Inventory of Authorized and Unauthorized Devices.
- CSC 2: Inventory of Authorized and Unauthorized Software.
- CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers.

3.1 Establish standard secure configurations of your operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration in light of recent vulnerabilities and attack vectors.

Table 2: Top 5 controls for security expects, Center for Internet Security in the USA, New York

The next chapter presents a few instructions that the official Twelve Step groups or organizations shall follow [16] concerning what the citizens can do when cyber-incidents emerge.

3. Securing online pubic services

3.1 Online helpdesk

This charter presents the twelve steps from the 12step.org portal that helps the citizen with or without awareness cyber-security in the cyber-work all time.

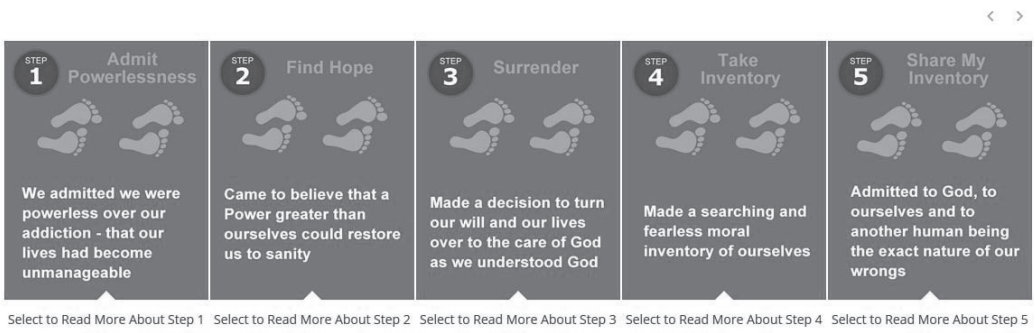

Figure 1: twelve steps, 12 STEP, http://www.12step.org

A few of the twelve steps are as follows [16]:

„Admit Powerlessness": The criminals have better finding, better researching and better resourcing ability than the country's citizens or the government's public servants. Cyber-criminals are hackers by profession so they have better equipment than the others employed. It is a weakness in the system, but may not be in despair.

„Find Hope": The citizens should not forget the hope of cyber-recovery. The citizens must to call for the person responsible for security in their organization who averts the incident and needs to restore the problem and the sanity of the users and reduce the feeling of powerlessness.

„Surrender": In fact the cyber assemblers help and actually do something to change which approaches are really destructive rather than constructive.

„Take Inventory": It has got to make a data backup if not at all time but at least regularly.

„Create the ISMS": In the high priority organizations or the governments' organizations it is obliged or recommended to create the Information Security Management System to effectively run the Information System. The ISMS rules give the instructions for the required level of information protection in the organization. The instructions for the work of citizens are included in the information system and for the internal audit of system. The ISMS doesn't work without the rules and the internal and external audit. There is a never ending stream of known-knowns that need to be continually addressed and promptly addressed.

„Meditate": This is the term in the information technology landscape which is the reflection time vital to improve, to understand and to know the risk landscape.

„Help Others": It has got to share the research results, the tutorials, the user's manuals with the partners, the vendors, the family members and the friends or the wider social circle, so that it can improve the interconnectivity of all collective devices.

3.2 Online helpdesk with cyber-devices

Today various forms of identification are widely found in test systems using different methods. System information tools have been researched whether they are able to discover a detailed network topology, hardware and software inventory. So it could provide us extremely detailed information not only about network, but hardware and installed software as well.

In the last few years Information Research were helped and improved materially by the color and a great many independent technical assessments of system (System Testing) and software development projects. Yearly there is a big number of utilities which are endorsing to explore the increasing scrutiny of IT Tools, the more comprehensive Network, Hardware and Software details.

The full Network Inventory making and monitoring IT Device Manager and Administrator System and Application shall endeavor to get close to Operating Systems Kernel, to collect a multitude of physical and logical Information, to analyze with different parameters, and to make feedback for the users, the system administrators or the hardware items factories. They do all this without any physical breakdown into pieces.

In this chapter the solutions are discussed that can help to collect most of the information related to the particular infrastructure including network topology, hardware and software elements as well. This information set is one of the main sources if we would like to estimate the security or the vulnerability risk of the infrastructure. The main advantage of our approach is that it focuses on IT security and the main purpose of information gathering is to improve the security level and decrease the risk related to it.

One of the most important areas of IT systems is the computer network, so a security analysis of network security is very important. By the network security investigation what should be considered is not only the endpoints but also the network security-relevant network devices, also known as security gateways, as well as the designed topology. Most of these are available in some form for companies. In addition, the test criteria were the type of network topologies – that are physical or logical –, the number and type of security gateways (LAN or WAN).

The network security testing has been influenced by the network services and network topology not only, but by all the endpoints features too. If a network endpoint can't be vulnerable by network services, it doesn't mean that the application of the endpoint can't access through the network services. Such application has security breaches. It is necessary to the network and applications System Information Tool to scan the more information about the endpoint. [17]

Security Vulnerabilities may be in plugin that is innocent-looking utilities. The user can give out the data by e-mail, on phone (GSM, 3/4G) or Internet/WiFi or Internal Network communications or other input data too. The Software Vulnerabilities are called the Vulnerable Operating Systems and Databases, Security updates or Faulty Application. The IT Prevention and Protection Method can reduce bad encryption, weak protection (viruses and spyware), the incorrect cleaning or weak passwords.

The result's system inventory is a report that includes the different network and hardware parameters and software environment parameters, which can help to find the network and system vulnerability. The more network and hardware detection applications usually are (more exactly system inventory) suitable for there, therefore the set of test described in this manuscript focus

exclusively the popular system inventory and their capable comparison, so the more distributions are found for the project.

Hardware and software inventory detailed by AIDA64 Network Audit from Windows platforms client connected to the corporate network is shown in Figure 1. This application is supported by command-line switches, creating inventories automated, which can make reports of the collected parameters from all the Network's devices, the PCs on the Network, shown in Figure 2. This AIDA64 Network Audit is compatible with all 32-bit and 64-bit Windows editions, including Windows 8.1 and Windows Server 2012 R2 too.

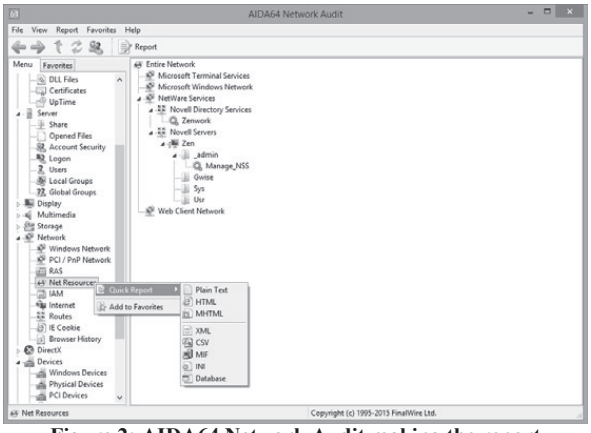

Figure 2: AIDA64 Network Audit making the report

Malware can be filtered with applications monitoring the system; their run can be spotted more easily. Naturally the appropriate and necessary utility can help the protection. Known as NOD32 ESET Endpoint Antivirus controls antivirus, antispyware and it securely supervises the operating system. This application has to keep the continuous control under the system and it has to run the virus definitely database daily so that the system can be safe. So this type of system controlling can slow down the full system and use better the resources, most of the time when it is most needed (for example data request). Of course the behavior of the system components and the monitoring can be optimized, so the most infection on the PC can be avoided. Without the systematic full system monitoring the system and their applications running slow down.

On behalf ESET spol. s r.o. the NRC marketing research and advisor Ltd. carried out the marketing research which was investigated behavior of the Hungarian Internet users with online survey, multilevel stratified and random sampling. The sample is a representative data of the people age between 18 and 69, who is at least a weekly on the Internet according to gender, age group, educational attainment and residence type. More than one million Hungarian visits knowingly the infected Web pages who gets to clear alert from the virus support before. One in ten adults, the 15 percent of the men or the 6 percent of the women switch off the security software on PC to want to access a file that is blocked by the anti-virus. Young people are particularly at risk (Figure 3). The 17 percent of the 18-29 years old usually switch off the security software on PC to want to open an infected file and the 12 percent of the 18-29 years old usually switch off the security software on PC to want to visit an infected WEB site.[18]

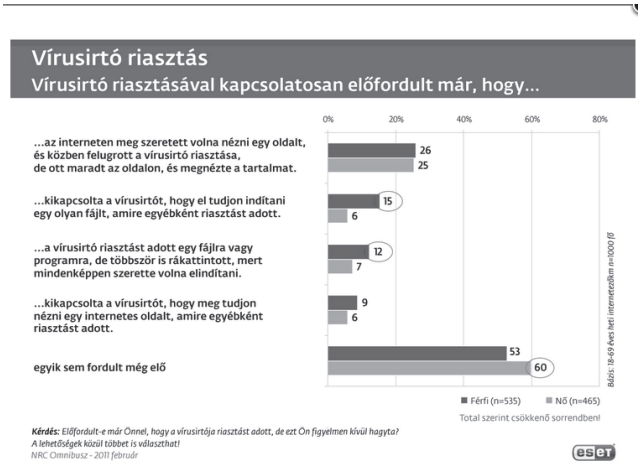

Figure 3: ESET, Hungarian Internet marketing research

There is another trap: the monitoring system made with good publicity but with the incorrect quality and the operating system used it. The Malware could be given access, it takes advantage of the system's weakness, it gets the data of the system and the user, phishing takes place.

The different types of system data can be collected in order to make complex statistics and the benchmarking system and the security risk testing system. The gained data can be compared with the data of the other operating system. Assessing the queered data the vulnerabilities of the system can be determined, the sensibility of the given data and the possibility of the good or bad using. The applications with the wrong-way used data can lead to Malware that can make use of the vulnerability of the system. The operating system has given out the most valuable information that runs on the PC or on the Mobile device (AIDA64) too.

The type and content of the data tracking can be difficult. The security risk and the number of the vulnerability can be lowered with the security rules and the security cases can be prevented. The very important security keys are Confidentiality, Integrity, Availability and their rules. [18]

4. Public servant awareness of their own vulnerability to cyber-threats

This chapter presents the result of test which was made by citizens' Public Service at an e-learning university system between October and November 2016. The test was written in December 2016. The constructive of strict information security rules help the citizens to understand the relevance of the rules. They are not aware of the need of information security. The other practical guide is the awareness of social engineering attention the ways that the organization don't be the victims of a possible social engineering attack.

On the Hungarian National University of Public Service the adult's information security teaching is followed by the year 2013 L. Hungarian Law [15]. One of the methods is the learning or orientation of the country's citizens or government's public servants where the citizens can get the information from the IT vulnerability or potential attack, the information security risk, the business continuous planning on the information security landscape or the information security rules by the teaching. On such as teaching the students wrote a test about their information security knowledge.

In the research the number of participants' is 42—there are IT security directors (18%), IT security managers (35%), persons responsible for data protection and jurists (2%), IT security experts (10%), IT engineers (5%) they are called IT experts.

The participants of the were IT experts age between 30 and 58, 66 percent age between 40 and 58 and 33 percent age under 40. 90 percent are male and 10 percent are female. 70 percent live in Budapest or Pest country and the rest live in the province. They are graduates.

The aim of the survey is to make statistics of the information security awareness, the information security practice, the knowledge of the Hungarian rules and the knowledge of the organizations structure and rules in the Hungarian Public Service. The survey of theme is the knowledge of the Hungarian Information Security Law in Public Service (IBTV) [3], obligation of the organization and rule with the IBTV, information security questions, IT risk analysis plan and functions. The IT experts corrected the test in the University where very interesting summary documents were made.

15 percent of the participants were excellent (90-100%), 70 percent good (75-90%) and 15 percent implemented the task at a medium level. The result were not influenced by the participants' age, gender or habitation, rather it was influenced by the work experience, the graduate and on the workplace loaded position.

The directors, the managers or jurists could give excellent answers to the question about the knowledge of the Hungarian rules and the knowledge of the organizations structure and rules in the Hungarian Public Service, and they could give weak answers to the question about IT themes. Even so they could implement the job very well. The IT engineer usually has not sufficient competence of organizational structure or rules. The engineers had excellent IT security practice, so they could answer the IT security exercise or questions very well.

The overall conclusion of the following discussion with the participants was that the IT security awareness should further develop in the Hungarian society. In the organization where the management is not engaged with the IT security, the IT rules of organization or Information Security Management System is only red tape documentation. Most of the IT experts consulted, according to the Hungarian IT control internationally advanced standards, believe much farther forward than the development of the use of the IT infrastructure.

On the other hand, from the test result it can be diagnosed that the interface is weak between IT regulation and IT practice. Both do not completely understand each other's language.

5. Conclusion

This paper outlines cyber-security which is a really broad area of information technology. It deals with average or medium vulnerability in an organization, citizens' identification, cyber-device and the information rules. The identification of the weakest links is indispensable in this context. The citizens who live in the country or work in the government's public service, their health, ill or behavior, their position in an organization, their professional experience are influential factors in the information security research. The citizens' health, ill or behavior causes real attention, because it influences the other component as well. The really important thing is the users' control without control which can occur from vulnerability to treatment, from attack trial to incident. It is an opportunity for cyber-crime and hackers wait for a chance.

Even the most advanced information technology and IT security system, the best IT professional, the most effective management in an organization, the best regulatory systems are useless if the citizen is the weakest link in the system who is keeping his/her own best interests in his/her mind, eliminates the Defence points and knowingly makes the system vulnerable. In the existing IT system the damage can be measured. In most cases it can cause completely irreparable damage. There is always an additional loss.

Citizens should be made aware on a regular basis of IT opportunities with the eventuating dangers and the caused damage too. The keyword is the systematic training and awareness. A single instruction is not enough, but information safety awareness for both a country's citizens and a government's public servants should be continuously improved.

6. References

[1] KOLKMAN, M.J. et al: Mental model mapping as a new tool to analyse the use of information in decision-making in integrated water management, Physics and Chemistry of the Earth, 30(4-5), 2005, pp. 317-332.

[2] HÖPPNER, C., Buchecker, M., and Bründl, M.: Risk communication and natural hazards. CapHaz project. Birmensdorf, Switzerland, 2010.

[3] GRANGER, S.: Social engineering fundamentals, part I: hacker tactics. Security Focus, December, 18, 2001.

[4] KROMBHOLZ, K., HOBEL, H., HUBER, M. and WEIPPL, E.: Advanced social engineering attacks. Journal of Information Security and applications, 22, 2015, p. 113-122.

[5] ORGILL, G. L., Romney, G. W., Bailey, M. G., & Orgill, P. M.: The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. In Proceedings of the 5th conference on Information technology education, 2004, October, pp. 177-181.

[6] PhishMe 2016 Enterprise Phishing Susceptibility and Resiliency Report (2016). PhishMe. available at: https://phishme.com/project/2016-phishing-susceptibility-report/

[7] SCHULLER: Az emberi tényező vizsgálata az információbiztonság, a személy- és vagyonvédelem, valamint az épületkiürítés területein, Nemzetközi Közszolgálati Egyetem, 2015.

[8] 1035/2012. (II. 21.) kormány határozat, Magyarország Nemzeti Biztonsági Stratégiájáról, 2012.

[9] 2013. évi L. törvény, az állami és önkormányzati szervek elektronikus információbiztonságáról, 2013.

[10] THE FINANCIALS TIMES, USA, New York.

[11] TÖRLEY, Közigazgatás - szervező hallgatók információbiztonság – tudatossága, Nemzetközi Közszolgálati Egyetem, 2016.

[12] ESET Magyarország: A kíváncsiságunk fertőz, 2011, http://www.eset.hu/hirek/kivancsisagunk _fertoz?back=/hirarchivu m%3Fpage%3D9 – State: 1. December, 2016.

[13] SANS INSTITUTE, CIS Critical Security Controls, https://www.sans.org, – State: 20 December, 2016.

[14] THE CENTER FOR INTERNET SECURITY, SECURITY CONTROLS, https://www.cisecurity.org, – State: 20 December 2016.

[15] https://www.owasp.org/index.php/Top_10_2013-A6-Sensitive_Data_Exposure, – State: 20 December 2016.

[16] 12 STEP, http://www.12step.org, – State: 20 December 2016.

[17] LEITOLD, F., et. al.: Testing endpoint protections against malicious URLs on social media sites, v 1.0, September 4, 2013, Veszprog Ltd, CheckVir.

[18] LEITOLD, F., et. al.: Combining commercial consensus and community crowd-sourced categorization of web sites for integrity against phishing and other web fraud,- 2014, Veszprog Ltd, CheckVir.

[19] ILLÉSSY, M., NEMESLAKI, A. and SOM, Z.: Elektronikus információbiztonság-tudatosság a magyar közigazgatásban, 2014.