

Nemeslaki, Andras; Sasvari, Peter

Book Part — Published Version

Empirical Analysis of Information Security Awareness in the Business and Public Sectors of Hungary

Suggested Citation: Nemeslaki, Andras; Sasvari, Peter (2015) : Empirical Analysis of Information Security Awareness in the Business and Public Sectors of Hungary, In: Balthasar, Alexander Golob, Blaž Hansen, Hendrik König, Balázs Müller-Török, Robert Prosser, Alexander (Ed.): Central and Eastern European eDem and eGov Days 2015. Time for a European Internet?, ISBN 978-2-85403-308-0, Österreichische Computer-Gesellschaft, Wien, pp. 405-418, <http://193.6.1.94:9080/?docId=20900>

This Version is available at:

<https://hdl.handle.net/10419/110229>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

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

Time for a European Internet?

books@ocg.at

Band 308

Wissenschaftliches Redaktionskomitee

o.Univ.Prof.Dr. Gerhard Chroust

Univ.Prof.Dr. Gabriele Kotsis

Univ.Prof. DDr. Gerald Quirchmayr

Univ.Prof. DDr. Erich Schweighofer

o.Univ.Prof.Dr. Peter Zinterhof

Univ.Prof. Dr. Jörg Zumbach

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

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

Time for a European Internet?

Conference Proceedings

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

Druck: Druckerei Riegelnik
1080 Wien, Piaristengasse 19

ISBN 978-2-85403-308-0

Co-Organisers:



www.ocg.at



uni-nke.hu



www.andrassyuni.eu



www.hs-ludwigsburg.de

BUNDESKANZLERAMT  ÖSTERREICH

INSTITUTE FOR STATE ORGANISATION
AND ADMINISTRATIVE REFORM

bka.gv.at/site/7764/default.aspx



legalpolicy.org



www.goforesight.eu

Partners:



www.okfbudapest.hu



www.kas.de

Sponsors:



www.bwstiftung.de

Gefördert von der BW STIFTUNG Baden-Württemberg



www.austrian.com

TABLE OF CONTENTS

1. Citizen Information	15
Citizen Information in E-Government.....	17
Roland Traunmüller, Andreas Krenmayr	
Croatian Central E-Government Portal: A Usefulness Analysis	27
Nikolina Žajdela Hrustek, Renata Mekovec, Goran Bubaš	
E-Governance in Georgia: Citizen-Serving, Informing and Empowering	43
Dennis Redeker, Tamar Iakobidze, Teona Turashvili	
2. Open Data.....	59
How Open Data is fuelling Co-Creation in Municipalities	61
Thimo Thoeye, Carina Veeckman, Pieter Colpaert, Mathias Van Compernelle	
Open Georgia: How Open Data Can Be Used As An Anti-Corruption Tool	71
Eric B. Jackson	
Comparing Open Budgets of Russia and Kazakhstan: Legal and Institutional Framework	77
Radomir Bolgov, Vitalina Karachay	
3. eID I	93
A browser-based JavaScript Solution for easy Smart Card-Access to European eIDs	95
Thomas Lenz, Bernd Zwattendorfer, Armin Hutzler	
eIDAS Regulation: A Step Forward?.....	105
Pavel Loutocký	
Reinventing Panopticon to Reconsider the Safety and Security vs. Privacy Issue Ontological Approach to Examine Surveillance	113
Hiroko Kudo	
4. eGovernment and the EU	125
Services Directive 2.0 – What we can expect and the challenges for public administration	127
David H. Fenner, Christine Leitner	
E-Cohesion How to Intensify European Fund Management by Electronic Services	141
Tamás Laposa	

Online market and tax avoidance – EU reacts, but additional problems arise.....	153
Oliver Sievering	
5. Smart Cities	163
What Kind of Citizen Participation is Needed for Smart Cities? Analysing Citizen Involvement in Japanese Smart Communities	165
Hiroko Kudo, Benoit Granier	
Smart City Platform Empowering People with Digital Services	183
Blaž Golob	
“Smart city” – Conception for local development?	191
Silvia Ručinská	
6. eID II	207
A Cross-Border Bank Account Opening Framework Using E-Government Technologies	209
Klaus Stranacher, Thomas Rössler	
Using eID Pseudonymity and Anonymity for Strengthening User Freedom in Internet	223
Blerim Rexha, Ehat Qerimi, Vehbi Neziri, Ramadan Dervishi	
Electronic identification and authorisation with focus on public administration in Hungary	233
Attila Kiss, Balázs Kónig	
7. eGovernment I	251
“E”-solutions – A new stimulus for cross-border governance?	253
Joachim Beck	
Research Agenda towards Structured and Sustainable Non-Bureaucratic Government	271
Alois Paulin	
Coexistence of the high-quality human resources and poor organisational capabilities	283
Csaba Makó, Miklós Illéssy	
8. Cyber Security I	297
Hungarian Trends in Password Usage in an International Comparison	299
Zoltán Som, Gergely Papp	
Detecting suspicious network activities and security related events with open-source software	315
Kálmán Hadarics, Ferenc Leitold	

Security impacts of community based software development	325
Gergely Mészáros	
9. European Citizens' Initiative	337
Reviewing the Regulation: The Future of European Citizens' Initiatives	339
Robert Stein, Gregor Wenda	
The European Citizens' Initiative – Proposed Modifications	349
Alexander Prosser	
The European Citizens' Initiative: Legal, technical and organizational requirements for any collection of online support	359
Robert Müller-Török, Birgit Schenk	
10. eGovernment II	367
Introducing digital long-term archiving for electronic government data: Lessons learned and recommendations	369
Hannes Kulovits, Andreas Rauber	
Human factors in the development of e-government within the public sector in Hungary	379
Mihály Csótó, Zoltán Rupp	
Evaluation of the Quality of Public Administration in Selected Towns of the Moravian-Silesian Region, the Czech Republic	393
Soňa Harasimová	
11. Cyber Security II	403
Empirical Analysis of Information Security Awareness in the Business and Public Sectors of Hungary	405
András Nemeslaki, Péter Sasvári	
Functions and perspectives of the right to be forgotten by a search engine	419
Matija Miloš	
E-safety, privacy and information security: Requirements in Public Administration	431
Csaba Krasznay, Gábor Törley	
12. Empowering Citizens	443
The Efficacy of E-Participation and Mobilization of Bias: A South Korean Experience	445
Heungsuk Choi, Kyoungsu Lee	
The role of the social media in civil initiatives	465
Péter Balkányi, Zsolt Orbán, Vitéz Nagy	

Campaigning for European Citizens' Initiatives: unexpected challenges and successes	479
Bengt Beier	
13. Transparent Government	489
Electronic legislation in the Czech Republic	491
Václav Stupka	
Active Citizenship – A Crucial Requirement for Open Governments in Europe	501
Lia-Alexandra Baltador, Mihai Baltador	
European e-consultation at work: The case of ISDS and its implications on multi-level governance in EU-US trade negotiations	509
Christine Leitner, Elisabeth Großschädl	
14. Age and Digital Divide	523
(Re-)Activating Senior Citizens – The Potential of Online Job Portals in Hungary	525
Janina Apostolou, Csilla Szentiványi, Martina Eckardt	
Social Media Platforms for Elderly – A General Privacy and Data Security Risk Analysis	537
Lukas Paa, Felix Piazzolo, Kristina Förster	
The Role of Cyber Diplomacy in the Fight Against Digital Divide in the EU	549
Helin Alagöz Gessler	
15. eEducation	563
Success of Online Enrolment System	565
Anna Orbán	
E-learning based education and e-skill development at the public service	579
Zsolt Orbán, Vitéz Nagy, Péter Balkányi	
16. eElections	595
An Introduction to a Formally Proved Independent Recount Solution for E-Voting	597
Alexander Scheidl	
Internet Penetration: A Way to Strengthening Electoral Integrity	609
Daniel Stockemer	
Mutual assistance and information exchange of tax authorities	621
Angelika Dölker	

PREFACE

Trust is an essential element in the acceptance of Internet-based services for transactions, whether that be in trade and commerce or with government agencies. In recent years, this trust has been undermined by a number of revelations that tended to decrease the general public's belief in electronic transactions. Internet services once trusted almost implicitly have been compromised. In addition, political statements are on record calling for a reduction of privacy in the Internet to more effectively fight criminal and terrorist activities. "Key escrow" and "government backdoors" are just two examples of these demands.

The Internet certainly has become part of a country's key infrastructure; however, it also creates a public sphere for transparency, democratic deliberation and decision making. It is therefore an essential element in the effort for good governance. In recent years, it has also become the means to interconnect devices creating new security and privacy challenges.

Due to the nature of the Internet, these questions can only be treated on a European level; does this mean to "Europeanise" the Internet? And if so, what would this involve and require? This conference and proceedings volume aims at providing new insight into the possible directions of ICT usage in the public sector with a particular view on fostering and promoting a common European identity.

The organizers of the conference are the Andr ssy University Budapest, the Austrian Computer Society, the Institute for State Organization and Administrative Reform in the Austrian Federal Chancellery, the Austrian Institute for European Law and Policy, the National University of Public Service Budapest, the GoForeSight Institute in Ljubljana and the University of Public Administration and Finance Ludwigsburg. The editors who are representing these institutions are most grateful for the support of our partners and sponsors of the conference and of this volume, especially the Austrian Federal Chancellery, the Konrad Adenauer Foundation, the Baden-W rttemberg Stiftung and the Austrian Cultural Forum Budapest.

The volume is dedicated to Prof. Johannes Pichler, head of the Institute of Development of European Law at the University of Graz and the Austrian Institute for European Law and Policy, Salzburg, on the occasion of receiving his emeritus status. Johannes Pichler has been at the forefront of European legal policy for many years. He has been a pro-active pioneer for each of the instruments of participatory democracy in the Union Treaty, from the ECI to the Civil Dialogues, including Multilevel Governance. Far from being "emeritus", Johannes Pichler is currently working on the implementation of the horizontal dialogue incorporated in Art 11 TEU.

The Editors

Budapest, Vienna, Ljubljana and Ludwigsburg, April, 2015

Programme Committee

Anderheiden Michael, Andrassy University Budapest
Awad Mohammed, American University of Ras al-Khaimah
Balthasar Alexander, Institute for State Organisation and Administrative Reform, A.F.C., Vienna
Beck Joachim, University of Public Administration Kehl
Bernhart Josef, European Academy Bozen
Bos Ellen, Andrassy University Budapest
Duma László, Corvinus University of Budapest
Eckardt Martina, Andrassy University Budapest
Eixelsberger Wolfgang, Carinthia University of Applied Sciences
Gajšek Miran, City of Ljubljana
Glidden Julia, 21st Century Consulting London
Golob Blaž, GoForeSight Institute, Ljubljana
Gourova Elissaveta, New Bulgarian University
Hansen Hendrik, Andrassy University Budapest
Harsági Viktória, Andrassy University Budapest
Holzner Matthias, State Ministry Baden-Württemberg
Kő Andrea, Corvinus University of Budapest
König Balázs, National University of Public Service
Krasznay Csaba, National University of Public Service
Kudo Hiroko, Chuo University
Kustor Peter, Federal Chancellery Vienna
Leiningen-Westerburg Alexander, postserver.at
Leitner Christine, Federal Ministry of Economy, Family and Youth
Lukac Irena, Center of Excellence in Finance Ljubljana
Makó Csaba, National University of Public Service
Müller-Török Robert, University of Public Administration and Finance Ludwigsburg
Nemeslaki András, National University of Public Service
Nešković Siniša, University of Belgrade
Okruh Stefan, Andrassy University Budapest
Pállinger Zóltan Tibor, Andrassy University Budapest
Paulin Alois, Vienna University of Technology
Pautsch Arne, University of Public Administration and Finance Ludwigsburg
Pichler Johannes, Austrian Institute of European Legal Policy
Pinter Róbert, Corvinus University of Budapest
Pirker Reinhard, University of Economics and Business Administration Vienna
Promberger Kurt, University Innsbruck
Prosser Alexander, University of Economics and Business Administration Vienna
Rauber Andreas, Technical University of Vienna
Rucinska Silvia, Pavol Jozef Šafárik University
Sasvári Péter, University of Miskolc
Schenk Birgit, University of Public Administration and Finance Ludwigsburg
Scola Dona, Former Deputy Minister of Information Technology, Moldova
Setnikar-Cankar Stanka, University of Ljubljana
Sievering Oliver, University of Public Administration and Finance Ludwigsburg
Simic Diana, University of Zagreb
Spichiger Andreas, Bern University of Applied Sciences
Szádeczky Tamás, National University of Public Service

Traunmüller Roland, Johannes Kepler-University Linz

Velikanov Cyril, Memorial Society, Moscow

Vincze Attila, Andrásy University Budapest

Weidinger Norbert, City of Vienna

Weiß Silke, Bundesministerium für Finanzen, AT

Wenger David R., Andrásy University Budapest

Wilding Michael, Eötvös Loránd University Budapest

EMPIRICAL ANALYSIS OF INFORMATION SECURITY AWARENESS IN THE BUSINESS AND PUBLIC SECTORS OF HUNGARY

András Nemeslaki¹, Péter Sasvári²

Abstract

Based on an empirical study of 300 employees in the public and business sectors of Hungary we found that the level of information security awareness can be considered good at corporations in the business sector, and at public institutions and state-owned organizations in the public sector. Employees need further training in this area mainly at medium-sized enterprises (employing less than 250 people), at for-profit local government organizations and at nearly a quarter of the local governments. Due to the low level of information security awareness, some parts of the micro and small-sized enterprises are in need of immediate changes in terms of organizational operations. The deficient knowledge of employees about information security gives room for grave concern at several local government organizations. Our sample also indicated that people with higher level of digital literacy show a higher level of information security awareness both in the business and the public sector.

1. Introduction

Security is a major concern for organizations which are present in the cyberspace. Many customers are hesitant to provide their personal information on the Internet due to the lack of privacy [10], and trust [13]. From an organization's perspective, lack of security knowledge and awareness on the part of employees is also a major problem. Numerous security risks such as viruses, worms, denial-of-service attacks, stolen passwords, human errors, behavioral misconduct, and authority violations are the result of a lack of security awareness. These risks are detrimental to the operation of any organization. As such, organizations need to be aware of these risks, dissuade individuals from committing risky acts, and deploy countermeasures such as deterrence, prevention, detection, and recovery.

Although many organizations have deployed hardware and software-based protections such as firewalls, proxy servers, anti-virus software, and password management, incorporating these technology-based solutions has not significantly decreased the security risks to organizations. In fact, risks and attacks are evolving to elude many current technology-based protections [3]. According to the 2005 Computer Crime and Security Survey conducted jointly by the Computer Security Institute and the Federal Bureau of Investigation, virus infection is still the most common security risk (73%). Insider abuse is now the second most common security risk (47%), more common than denial of service attacks (32%) [8]. Today's security problems are primarily due to the inadequate security awareness of users, which can be mitigated without the need for sophisticated security technologies, it seems like that human factor in security is equal, if not, more important than technology [6]. It is no use installing the most sophisticated safety devices to our information systems, protecting our corporate data with passwords and other tools of access protection if our users or our employees cannot or do not want to behave responsibly when using

¹ National University of Public Service nemeslaki.andras@uni-nke.hu

² National University of Public Service sasvari.peter@uni-nke.hu

these systems. The above statement is especially true for small and medium-sized enterprises, as central regulation of security which is systematically used by larger corporations is less typical of them [14].

Derived from these problems, and building on an empirical study executed in 2014 measuring information security awareness (ISA) amongst several hundred Hungarian public servants [18], we designed a research model to compare public and business sectors on ISA. Our research question was straightforward: What are the main differences in the Hungarian business and public sector organizations in terms of ISA using the SANS (Security Awareness Survey) [20].

2. The concept of information security awareness (ISA)

According to [2] ISA is defined as an employee's general knowledge about information security and his cognizance of the information security policy in the organization [2, page 532.] ISA is composed of general information security awareness and policy awareness. Since ISA plays such a pivotal role in lowering information security risks its increase in organizations is essential.

Information security is related to the protection of *data*, which are stored either in the form of symbols, writing or by other communication, *information technology* and other *electronic systems* [15]. Information security requirements can be divided into three categories [12]:

- a) *Physical security* is a protection against any threats occurring in the physical space, its major parts are the protection against natural disasters, mechanical protection, electronic signaling system, manned security, access control systems, surveillance systems, the power supply, the protection against radiated and conducted interference, air-conditioning and fire protection.
- b) *Logical protection* is a form of protection implemented in the electronic information systems by information technology tools and procedures (programs, protocols).
- c) *Administrative protection* is composed of organizational, regulation and control measures, supplemented by regular education on protection procedures (in relation to the adequacy of management systems) [21]. In order to achieve the appropriate level of information security and maintenance, it is needed to look beyond the physical and logical protection, and we have to manage the threats caused by the human factor as well. These threats can be traced back mainly to the lack of necessary knowledge and the low level of the awareness of the cause and effect relationships related to the information processing activities.

In the Hungarian context information security policies stem from a general Cybersecurity Strategy [9] and Cybersecurity Legislation [1]. In the public sector organizations' compliance and motivation should enforce these general policies. There is a conceptual understanding in the literature that both compliance and motivation of users/employees/civil servants can be achieved by raising policy awareness, systematic enforcement and regular maintenance of technological and human procedures [11]. Derived from this logic, our unit of analysis is the user and his/her information security awareness (ISA), since ISA is a key element of all security policies [2].

In this context, ISA is part of the organizational culture, it is a way of thinking and behavior which ensures that the employees of the organizations are committed to acknowledge the legitimacy of security measures, they abide them and they also make them known to others and enforce their

application. This culture is cultivated by focusing on the barriers preventing deepening ISA such as lack of computer skills, general security knowledge, limits of organizational budgets, little comprehension on the different responsibilities [19].

3. The research model of information security awareness

Our research design is based on the SANS model and questionnaire which was created by information security experts in the US in 2012 [20]. The questionnaire is aimed at measuring everyday user habits, assessing them by giving scores ranging from 1 to 5. Based on the aggregated scores, the respondents are classified into five risk categories:

- It is typical of the employees belonging to the *first category* that they are aware of the security principles as well as the dangers, they are well-educated, their everyday behavior meets workplace safety rules and guidelines.
- Employees found in the *second category* participated in some kind of information security training, they are also aware of the dangers, but do not fully follow the relevant safety principles and rules.
- Representing the group of average risk, those employees come under the *third category*, who are aware of the dangers and know that they should keep some basic safety principles but they are in need of further education on the subject. They do not recognize IT incidents and do not know what to do in such cases.
- The employees included in the *fourth category* are neither aware of the dangers and safety principles, nor of the security regulations in their organization.
- Finally, employees belonging to the *fifth category* are not aware of the dangers and do not comply with the security regulations, either.

In order to obtain a more detailed picture of ISA responses we separated the construct along three major dimensions [18]:

- **Organizational dimension** where the organizational habits and procedures are measured.
- **Individual dimension** where a general knowledge of the organization and working habits are measured and analyzed.
- **Infrastructural dimension** which includes the opinions on the environmental and IT state of the organization.

The research model for investigating ISA is summarized in *Figure 1*.

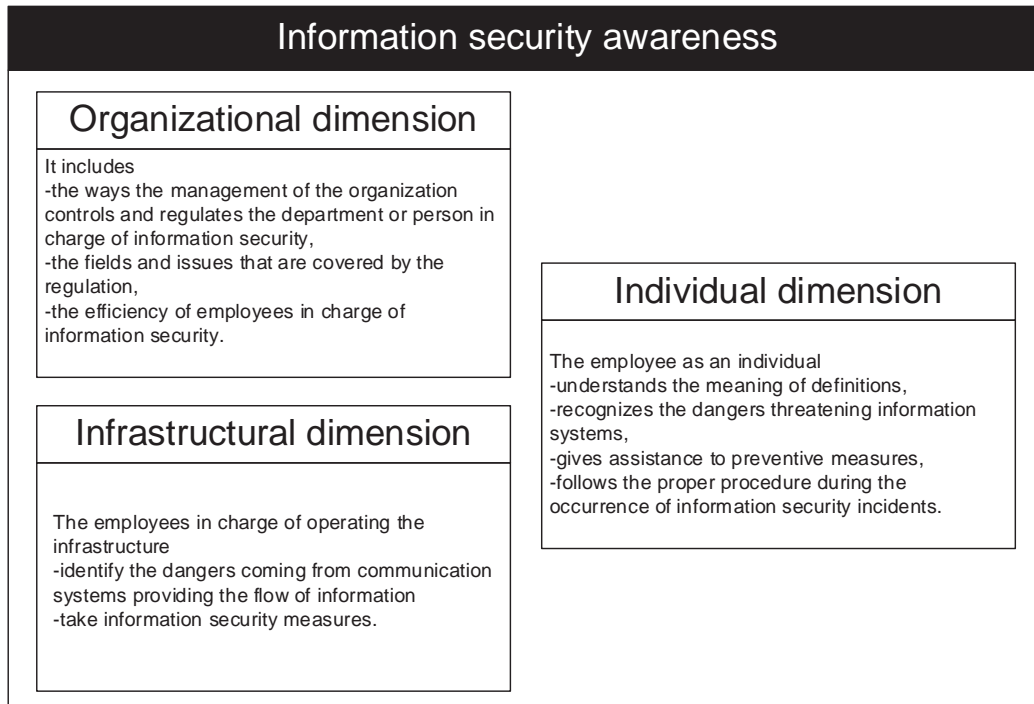


Figure 1 - The structure of the research model

Organizational dimension includes:

- the ways the management of the organization controls and regulates the department or person in charge of information security,
- the fields and issues that are covered by the regulation,
- the efficiency of employees in charge of information security.

Both external (eg. legislation, standards, policy impacts, market impacts and natural events) and internal factors (eg. regulations, the direct instructions of management, human resources management and control) have effects on organizational awareness [12].

Individual dimension measures IT knowledge, skills and abilities of the *employees*. In the specific case of information security awareness, it means that the employee:

- understands the meaning of the definitions,
- recognizes the dangers threatening the operation of information systems,
- gives assistance to preventive measures,
- follows the proper procedure in case of an information security incident.

The information *infrastructure* is another essential component of the information environment, which partly includes communication (network) systems, devices and resources providing information flow between local information environments, on the other hand it is also composed of

all the organizational tools and other resources which provide basic or value-added (information security, logistics etc.) services [17]. In view of the above, the infrastructural dimension also includes the employees in charge of operating the infrastructure who:

- identify the dangers originating from communication systems providing the flow of information,
- take the necessary information security measures.

Everything can be considered a source of danger or risk that causes a breach in information security or results in a non-desired change in the function of one or more components of the information system [16].

4. Methodology and data collection

The core instrument of our data collection method was

- the Security Awareness Survey (SANS) developed and used by Bond, Stephens and Piscitelli [20]
- and a questionnaire previously used in a query at the National University of Public Service and further improved by Illéssy, Nemeslaki and Som [18].

The level of digital literacy was measured and assessed by several questions relating to several areas in the questionnaire. In order to survey the use of network information technology, the knowledge on mobile network devices, as well as the length of Internet use were questioned. Hardware skills were determined by questions aiming at the knowledge about storage devices, and the duration of computer use. The level of software skills was measured by questions about the knowledge on computer installation and deployment. Finally, general information security knowledge was assessed by questions relating to computer viruses.

In terms of public organizations our respondents were categorized into 6 categories using the framework of Gajdushek defining public service in general [7]. According to this, public service, in its narrowest sense means only administrative offices whereas in its broadest sense it may refer to all the institutions of the public sector that is the three branches of state power organizations (legislative, executive and judicial bodies) but, in addition, it can also be extended to the armed forces, schools, hospitals, social services, public corporations or foundations performing public functions. To serve its function in the wider sense a public organization can be *non-profit*, and *for-profit* as well. Based on the narrow sense the public sector consist of the *central* and the *local government* organizations.

Responses from business organizations were categorized into 4 groups; *micro, small and medium-sized enterprises* and *corporations*.

The questionnaire was filled out by 316 persons altogether until April, 2014. The number of employed respondents was 120, while 196 of them were unemployed. Of the 120 employed respondents, 34 of them represented the business sector (eg. micro, small and medium-sized enterprises or corporations) and 86 of them were employed in the public sector (eg. public

institutions, state-owned organizations, local governments, organizations in local government ownership).

The responses according to the categories in public and business organizations are shown in *Figure 2*.

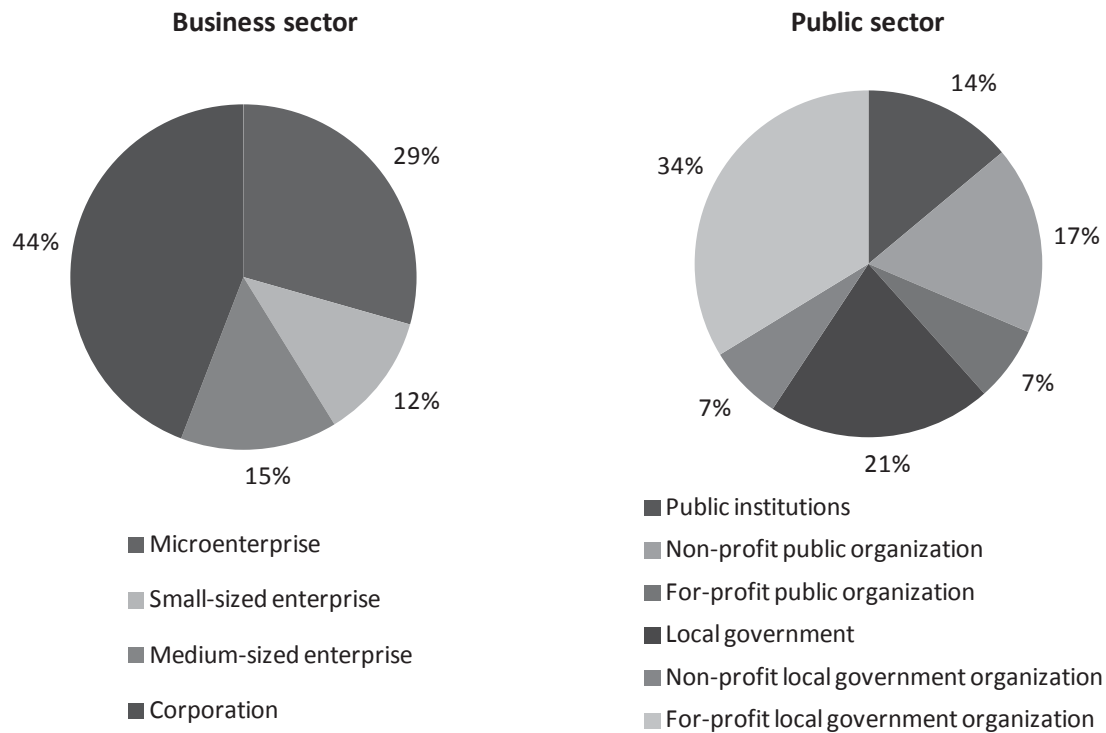


Figure 2 - The division of the respondents to the questionnaire on information security awareness

The questionnaire consisted of four parts:

- **Demographic questions:** in addition to the most important demographic data (eg. gender, year of birth, education level, income status), the respondents' IT skills were also questioned.
- **Questions on workplace:** if the respondent was employed, the sector and the region of their workplace were asked about as well.
- **Questions on information security awareness** were centered around the following issues: work organization and regulation, everyday use of skills related to information security, the use of IT tools and data management, general computer usage habits.

5. Analysis of results: the situation of ISA in Hungary in 2014

Looking at the findings in *Table 1* we can see that two types of organization - *public institutions* and *for-profit public organizations* - belong only to the safest first and second categories. Similarly good results are shown by *corporations* as well as *non-profit public organizations* in the sample. On the other hand, it has to be acknowledged that nearly 8% of the respondents from these latter groups belong to the third category representing average risk.

Worse rates can be found in the case of *medium-sized enterprises* employing less than 250 workers, *for-profit local government organizations* and *local governments* themselves. Nearly a quarter of the employees in these organizations would need further training in information security awareness. Finally, the last category includes those organizations where none of them gave a response belonging to the first risk category. Here, *non-profit government organizations* from the public sector, and *microenterprises* and *small-sized enterprises* employing less than 50 workers can be found

Record	Ranking	Type	First category	Second category	Third category
High	1	For-profit public organization	40%	60%	0%
	2	Public institutions	27%	73%	0%
Good	3	Corporation	31%	61%	8%
	4	Non-profit public organization	22%	71%	7%
Average	5	Medium-sized enterprise	33%	33%	34%
	6	For-profit local government organization	30%	44%	26%
	7	Local government	7%	71%	22%
Low	8	Non-profit local government organization	0%	67%	33%
	9	Small-sized enterprise	0%	100%	0%
	10	Microenterprise	0%	78%	22%

Table 1 - The qualification of ISA in the Hungarian business and public sector

5.1. The organizational dimension of ISA

In *Table 2*, we show that in the organizational dimension for type of organizations - *for-profit public organizations*, *corporations*, *public institutions* and *non-profit local government organizations* - got into the top two risk categories.

Ranking	Type	First category	Second category	Third category	Fourth category
1	For-profit public organization	0%	100%	0%	0%
2	Corporation	15%	85%	0%	0%
3	Public institutions	9%	73%	18%	0%
4	Non-profit local government organization	0%	100%	0%	0%
5	Non-profit public organization	7%	57%	36%	0%
6	For-profit local government organization	22%	39%	26%	13%
7	Medium-sized enterprise	0%	67%	33%	0%
8	Small-sized enterprise	0%	50%	50%	0%
9	Local government	0%	50%	43%	7%
10	Microenterprise	0%	33%	44%	22%

Table 2 - The qualification of ISA in the Hungarian business and public sector (organizational dimension)

100% of the *non-profit public organizations*, *local governments* and *non-profit local government organizations* reported that they maintain an IT security department. High scores were given by *for-profit public organizations* and *for-profit local government organizations* (83%) as well. The

highest score in the business sector in terms of IT security function was achieved by corporations (93%). They were followed by *medium-sized enterprises* with fewer than 250 employees (80%) and *small-sized enterprises* (75%). The lowest rate of 40% was produced by *microenterprises* having low level of capital and human resources for security.

It was somewhat unexpected that some of the *local governments* and *for-profit local government organizations* got into the fourth risk category, which can be alarming with respect to information security.

An illustrative element of the individual factor has been the issue *whether there is a regulation on the use of IT tools* or they apply general rules which also include the use of IT tools. On average, a quarter of those surveyed could not say whether there were such policies in their workplace. This rate has reached 40% in the case of public institutions and local governments. More than 80% of microenterprises, nearly two-thirds of the local governments and half of the organizations in local government ownership reported that they did not apply any regulation relating to information technology. On the other hand, two-thirds of the corporations and non-profit public organizations used specific IT regulations and guidelines. This rate was 20% in public institutions and 30% of them used general regulations including the use of IT tools.

5.2. The individual dimension of ISA

When examining the individual dimension we measured the general IT knowledge of the respondents. This is largely depending on the practice the employees which they have earned during their employment. The respondents mentioned an average duration of 12 to 20 years of computer use. In terms of using the Internet, however, the average duration had been between 8 and 15 years both in the business and public sector. Focusing on the daily use of computer, we can conclude that employees working in every surveyed enterprise and institution spend between 5 to 8 hours a day in front of their computer on average. This result is important, because regardless of the workplace of our sample respondents', they have similar practice and experience in terms of IT use.

Scores in the first and second ISA categories exceeded 66% in the case of the *medium-sized enterprises*, *non-profit public organizations*, *public institutions*, *for-profit public organizations* as well as *corporations*. It is alarming though, that 7-98% of employees working at *corporations*, *for-profit local government organizations* and *non-profit public organizations* are not aware at high levels of the threats and safety principles.

Ranking	Type	First category	Second category	Third category	Fourth category	Fifth category
1	Medium-sized enterprise	67%	0%	33%	0%	0%
2	Non-profit public organization	29%	64%	0%	7%	0%
3	Public institutions	36%	45%	18%	0%	0%
4	For-profit public organization	20%	60%	20%	0%	0%
5	Corporation	38%	31%	23%	8%	0%
6	For-profit local government organization	39%	35%	17%	0%	9%
7	Microenterprise	0%	78%	22%	0%	0%
8	Local government	7%	64%	29%	0%	0%
9	Small-sized enterprise	0%	50%	50%	0%	0%
10	Non-profit local government organization	0%	67%	0%	33%	0%

Table 3 - The qualification of information security awareness in the Hungarian business and public sector based on the individual dimension

In the case of *for-profit local government organizations* this 9% of the respondents fell into the fifth category.

All in all, the lowest scores were measured in microenterprises, small-sized enterprises, local governments and for-profit local government organizations during the examination of information security as part of the individual dimension.

An interestingly characteristic element in the individual dimension has been the proportion of employees *voluntarily granting their company passwords* to other users. Respondents from public institutions and corporations gave their company passwords to other users in the largest rate (40%). In contrast, employees working in microenterprises, small and medium-sized enterprises, and non-profit public organizations were the most reluctant to give their company passwords to others (10%). A slightly higher rate, 16% was found in the remaining organizations in the sample.

A corresponding question to the previous one was whether *the respondent's boss had ever asked for their company password* or not. Most surprisingly, such a case has already occurred at almost half of the corporations. A low prevalence of 7% was experienced in the case of local governments and medium-sized enterprises. The rates were measured between 10 and 17% in the remaining organizations.

5.3. The infrastructural dimension of ISA

In the infrastructural dimension of ISA *public institutions* and *for-profit public organizations* achieved the best ratings, followed by the medium-sized enterprises which could reach a good rate of responses falling into the first category (*Table. 4.*) However, in their case, due to a third of their employees' responses falling into the third category means that in these organizations we might expect more awareness. The same rate was 8% in the case of *corporations* which was very similar to the rate measured in *non-profit public organizations* (7%). A 7% of these latter institutions were not aware of the basic principles and safety hazards (fourth category).

Ranking	Type	First category	Second category	Third category	Fourth category
1	Public institutions	36%	64%	0%	0%
2	For-profit public organization	20%	80%	0%	0%
3	Medium-sized enterprise	67%	0%	33%	0%
4	Corporation	38%	54%	8%	0%
5	Non-profit public organization	36%	50%	7%	7%
6	For-profit local government organization	35%	48%	17%	0%
7	Microenterprise	22%	78%	0%	0%
8	Local government	29%	50%	21%	0%
9	Small-sized enterprise	0%	100%	0%	0%
10	Non-profit local government organization	0%	100%	0%	0%

Table 4 - The qualification of information security awareness in the Hungarian business and public sector based on the infrastructural dimension

A fifth of the employees in local governments in our sample would also need more training in the field of ISA.

In the responses given to a number of questions on infrastructural dimension, a lack of knowledge or the overvaluation of some infrastructural parts have appeared quite frequently. Such a statement can be, for instance, according to which the information stored in the employee's computer is of no value to hackers.

More than a third of the employees working both in the business and private sector were convinced that their computers were not targeted by hackers. Even higher rates in the business sector than that were found only in *microenterprises* (50%) *corporations* (40%). Every four person working in small and medium-sized enterprises thought that they were not a target of this type of attacks.

55% of the employees working in *local governments* believed that the data on their computers were not interesting to others. Among the studied organizations in the public sector, 90% of the employees reported that the information on their workstations might be of interest to hackers.

5.4 Digital literacy and ISA

It *Figure 3*, we compared how the ISA scores of public and business organizations compare when we group them according to level of digital literacy.

We classified digital literacy into five categories [4]:

- **Excellent** if users recognize information needs, they have long shown excellence in managing IT networks, they have reached a high level of hardware and software management, and finally they are well aware of the dangers and they can also protect against them.

- **Good** if the users almost always recognize their information needs, they use network communication devices, they are excellent at certain areas of hardware and software management, and also familiar with the field of information security.
- **Average** if the users need some help to recognize their information needs, they use network communication devices with assistance, they suffer from some shortcomings in the area of hardware and software management, they make occasional mistakes in the area of information security.
- **Bad** if the users do not recognize their information needs because of lack of training and experience, they are not able to use network communication devices sufficiently, they have great deficiencies in the field of software and hardware management, and they are incapable of identifying network threats and dangers.
- **Very bad** if the users have no idea about their information needs, they lack even basic knowledge on the use of network communication, and they lack any software and hardware skills.

The natural hypothesis is that the higher digital literacy one has, the more he/she is aware of the risks of ICT use. Population of responses in the categories of *Figure 3*. somewhat indicate this assumption. If we look at for instance the two extreme cases 100% of the lowest digital literacy respondents fall into the third ISA category, while 75% of the top literacy skilled employees fall into the best ISA grade. *Figure 3*. also shows us, that this assumptions requires more thorough research or methodology, since in the case of business organizations we only see a few hits in the top ISA score regardless of our measured ICT skills (8% and 7%).

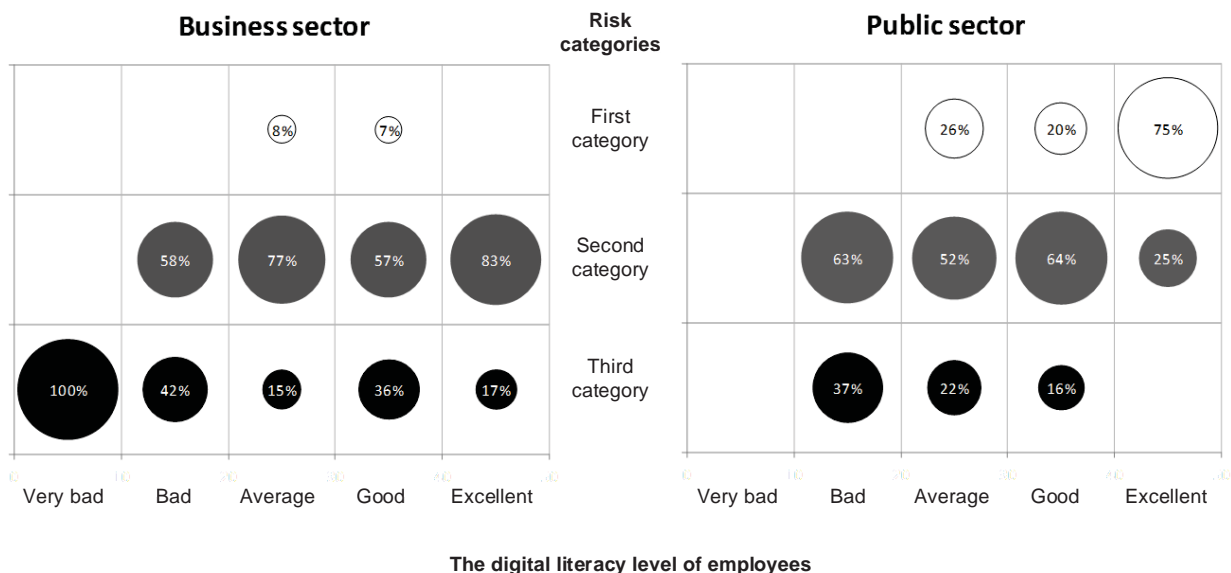


Figure 3 - The connection between global risk categories and the digital literacy of employees

6. Conclusions

In our exploratory study we intended to compare the conditions of information security awareness in the business and the public sector.

Generally, in the public sector our sample has shown higher ISA especially in the case of *public institutions* and *state-owned organizations*. The employees working in these organizations reported awareness of the possible dangers and safety principles, already participated in some information security training, they seemed to be well informed and follow the relevant safety principles and rules.

A fairly good level of information security awareness was found in *corporations* in the business sector and in *non-profit public organizations* in the public sector. The employees have already participated in some information security training, they are aware of the dangers but they need further education on the subject. A minority of the employees did not seem to notice that their computer was attacked, a third of them either voluntarily or forcibly gave their company password to others, and thought that their computers were secured against data theft.

The level of ISA can be regarded average in *medium-sized enterprises*, *local governments*, and *for-profit local government organizations*. Employees working there are aware of the dangers and know that some basic safety principles should be met although they are in need of further education on the subject.

A poor level of information security awareness was measured in *microenterprises* and *small-sized enterprises* in the business sector, and *non-profit local government organizations* in the public sector. The employees belonging to this group are partly aware of the dangers and they know in most cases that certain security principles should be met but they are in need of further education on the subject. Some of them are neither aware of the dangers and safety principles, nor of the security regulations in their workplace at all.

In our sample we observed that employees with higher digital literacy in the public sector fell into a lower risk category than their peers in the business sector. However the relationship of ISA and digital literacy need further testing.

Finally we need to point out the limitations and further directions of our study. As we aimed exploration in the area of ISA, the theoretical basis of our constructs need a more elaborate foundation, and also the refinement of the organizational classification of the public and government sector. In this study our sample size has been limited skewing toward the public sector and not providing indications for appropriate representativeness of the populations in the organizations.

Improvement of these deficiencies indicate future research directions not only for the theoretical exploration of ISA but importantly to support strategies for policy makers in order to better prepare employees for working in the new environments of the growing cyberspace.

7. References

- [1] ACT OF CYBER SECURITY AND CRITICAL INFRASTRUCTURE PROTECTION (Act No.L./2013), Magyar Közlöny, No.69. Vol. 2013. pp. 50241-50255
- [2] BULGURCU, B., CAVUSOGLU, H. and BENBASAT, I., Information Security Policy Compliance: An Empirical Study Of Rationality-Based Beliefs And Information Security Awareness, in: MIS Quarterly. Vol. 34. Issue 3. pp. 523-548, 2010
- [3] CLABURN, T., The Threats Get Nastier. IT threats are growing in number, sophistication, and ill intent. Think you've got them under control? Just wait till tomorrow. InformationWeek, Aug 29, 2005. (in <http://www.informationweek.com/story/showArticle.jhtml?articleID=170100709>)
- [4] CETF ICT Digital Literacy Initiative (2008): Consensus Document, 2008. november (in <http://www.ictliteracy.info/rf.pdf/California%20ICT%20Assessments%20and%20Curriculum%20Framework.pdf>)
- [5] CHEN, C. C., SHAW R. S., and YANG, S.C., Mitigating Information Security Risks by Increasing User Security Awareness: A Case Study of an Information Security Awareness System, Information Technology, Learning, and Performance Journal, Vol. 24, No. 1 1 2006
- [6] DESMAN, M. B., The Ten Commandments of Information Security Awareness Training. Information Systems Security, January/February, 39-44. 2003.
- [7] GAJDUSHEK, GY., Közszolgálat. A magyar közigazgatás személyi állománya és személyzeti rendszere az empirikus adatok tükrében. (Public Service. Personnel system of Hungarian public administration in the framework of empiricak data) Budapest. KSZK 2008.
- [8] GORDON, L., LOEB, M., LUCYSHYN, W. and RICHARDSON, R., 2006 CSI/FBI Computer Crime and Security Survey. Computer Security Institute., 2006 (in http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf)
- [9] GOVERNMENT DECREE (1139/2013. (III.21.)) ont he Strategy National Cyber Security of Hungary (2013), Magyar Közlöny, No.47. Vol. 2013. pp. 6338-6341.
- [10] HOFFMAN, D. L., NOVAK, T. P., and PERALTA M., Building Con Trust Online, How merchants can win back lost consumer trust in the interests of e-commerce sales, COMMUNICATIONS OF THE ACM, April 1999/Vol. 42, No. 4. 1999.
- [11] KNAPP, K. J., FERRANTE, C. J., Policy Awareness, Enforcement and Maintenance: Critical to Information Security Effectiveness in Organizations, Journal of Management Policy and Practice. Vol. 13. Issue 5, p66-80. 2012.
- [12] KODAJ, K. (2013): A Nemzeti Elektronikus Információbiztonsági Hatóság. (Introduction to the National Electronic Information Security Bureau.)
- [13] LIU, C., MARCHEWKA, J. T., LU, J. and YU, C. Y., "Beyond Concerns: A Privacy-Trust-Behavior Intention Model," Information & Management (I&M), 42(1), pp. 289-304. 2005.

-
- [14] KÜRT ZRT., Informatikai biztonsági tudatosság oktatása, (Educating for information security awareness) 2014 (in <http://www.kurt.hu/megoldasaink/informatikai-biztonsagi-tudatossag-oktatasa/>)
- [15] MUHA, L., Az informatikai biztonság egy lehetséges rendszertana (Recommendation for a framework for information security) (in BOLYAI SZEMLE 17: (4) pp. 137-156.) 2008.
- [16] MUHA, L., Fogalmak és definíciók (Terminologies and definitions): 2.4. In Maha L. (szerk.) Az informatikai biztonság kézikönyve (Handbook of information security): Informatikai biztonsági tanácsadó A-tól Z-ig (Information Security Advisor, from A to Z)., Budapest: Verlag Dashöfer, 2004. pp. 1-37. 2004.
- [17] MUNK, S., Információs színtér, információs környezet, információs infrastruktúra, (Theater of information, information environment and infrastructure) Nemzetvédelmi Egyetemi Közlemények (Annals of National Defence) VI.:(2) pp. 133-154. 2002. (http://uni-nke.hu/downloads/konyvtar/digitgy/20022/vszt/munk.html#_ftn35)
- [18] NEMESLAKI, A. and ILLÉSSY, M., Information Security Awareness in the Hungarian Public Sector: Result of an Empirical Study, CEEeGov Days 2014, eGovernment: Driver or Stumbling Block for European Integration? Proceedings of the CEEeGov Days, May 8-9, 2014 Budapest, 2014.
- [19] SHAW, R. S., CHEN, C. C. and HARRIS, A. L., The impact of information richness on information security awareness training effectiveness, Computers and Education, Vol. 52. No. 1. pp. 92-100. 2009.
- [20] TRENTON, B., CORTNEY, S., and DAVE P., Security Awareness Survey, 2012.
- [21] VINÇOTTE INTERNATIONAL HUNGARY Kft. (2013): A Vincotte komplex megoldáscsomagja a közigazgatásban és a kormányzati szférában működő szervezeteknek (The complex solution package of Vincotte for organizations operating in public administration and government) (in <http://www.vincotte.hu/Tanusitas/Informaciobiztonsag-a-kormanyzati-szektorban>)