AARMS Vol. 14, No. 1 (2015) 63–78.

# Old Monarchy in the New Cyberspace: Empirical Examination of Information Security Awareness among Austrian and Hungarian Enterprises

SASVÁRI Péter,[1] NEMESLAKI András,[2] Wolf RAUCH[3]

*Information security awareness is part of organizational culture, a way of thinking and behavior which ensures that the employees of the organizations are committed to acknowledging the legitimacy of security measures, they abide by them and they also make them known to others and enforce their application. After collecting empirical data from 280 Austrian and 470 Hungarian employees of different companies we concluded that the level of information security awareness of managers and employees in the Austrian and Hungarian business sector depends on company size. The level of this type of awareness can be regarded as good in the case of corporations both in Austria and Hungary. A good level of information security awareness was observed among the Austrian medium-sized enterprises. However, in a fifth of their Hungarian counterparts, the employees need further trainings in this area. Security problems can be traced back to poor organization at a fifth of the Austrian small-sized enterprises, a third of the Austrian microenterprises, and three-quarters of the Hungarian microenterprises. In 20% of the Austrian and Hungarian enterprises, employees have distressing gaps in their knowledge in this area, furthermore, it can also be concluded that employees with higher digital literacy have a higher level of information security awareness in Austria compared to the Hungarian business sector.*

**Keywords:** *Information security awareness, Austria, Hungary, Business sector, Enterprises*

## Introduction

As our information society develops, in other words, as more and more individuals, companies and governments use information communication technologies (ICT) – computers, information systems, mobile phones, intelligent sensors, internet applications, etc. – the more we are exposed to the new challenges of cybercrime, cyberterrorism, cyber espionage and – as far as governments are concerned – even to cyber warfare. [8] [19] The concept

1 National University of Public Service, Faculty of Public Administration, Institute of E-Public Service Development, Associate Professor, E-mail: sasvari.peter@uni-nke.hu

2 National University of Public Service, Faculty of Public Administration, Institute of E-Public Service Development, Full Professor, E-mail: nemeslaki.andras@uni-nke.hu

3 Karl-Franzens-Universität Graz, Institut für Informationswissenschaft und Wirtschaftsinformatik, Full Professor, E-mail: wolf.rauch@uni-graz.at

of the famous second part of the Terminator series "Judgment Day" and other Hollywood "end-of-the-world" movie scenarios where computer systems are attacked are not fictions anymore; there are real world examples of government conflicts exploited online, corporations' hacked for steeling commercial information, and hundreds of thousands individual bank accounts compromised. [11] Kovács and Krasznay in their visionary article describe how the so called critical infrastructure – energy, water, transportation, electronic media and commerce – could collapse in Hungary if she was exposed to a systematic cyberattack from hostile enemies. [12]

The answer to these new ICT challenges are naturally new technologies, but regardless of the fact that many organizations have deployed hardware and software-based protection such as firewalls, proxy servers, anti-virus software, and password management, incorporating these technology-based solutions have not significantly decreased the security risks of organizations. As some research has found, 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%), but insider abuse has come up to the second most common security risk item (47%), more common than denial of service attacks (32%). [6] Inadequate security awareness of users – the human factor in security – seems equal, if not, more important than technology. [5] [15] Anecdotal experiences of a leading training firm in Hungary show that these observations are 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. [13]

Our intention has been to contribute to this stream of research basically by providing empirical evidence for the relevance of information security awareness (ISA) in corporations. For increasing generalizability we have chosen companies of different sizes in Hungary and Austria, the research design has enabled us to compare ISA in two different yet similar economies. On the one hand Austria and Hungary have been closely integrated in the EU through their history, culture and intertwining business relations. On the other hand, both the level economy and information society are different in the two neighboring countries which according to our hypothesis impacts ISA.

The structure of the paper is as follows. First, we introduce the concept of information security awareness and our instrument to measure it. Then we describe the key characteristics of the Austrian and Hungarian information society together with the descriptive data of our company sample. In the third section we discuss the results of our surveys and finally we draw conclusions and suggest further extensions of our research model.

## *The Conceptual Model of Information Security Awareness*

According to Muha, *information security* is related to the protection of data that are stored either in the form of drawing, writing or by communication, information technology and other electronic systems, or treated in any other way. [7] [16] *Information security awareness (ISA)*, on the other hand goes beyond information security, it is part of the organizational culture, 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 by them and they also make them known to others and enforce their application. [2]

In order to measure the construct of ISA we use the work of Illéssy, Nemeslaki and Som who suggested dividing ISA into three main dimensions: [9]

- *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 opinions about the general security and concrete IT systems of the organization.

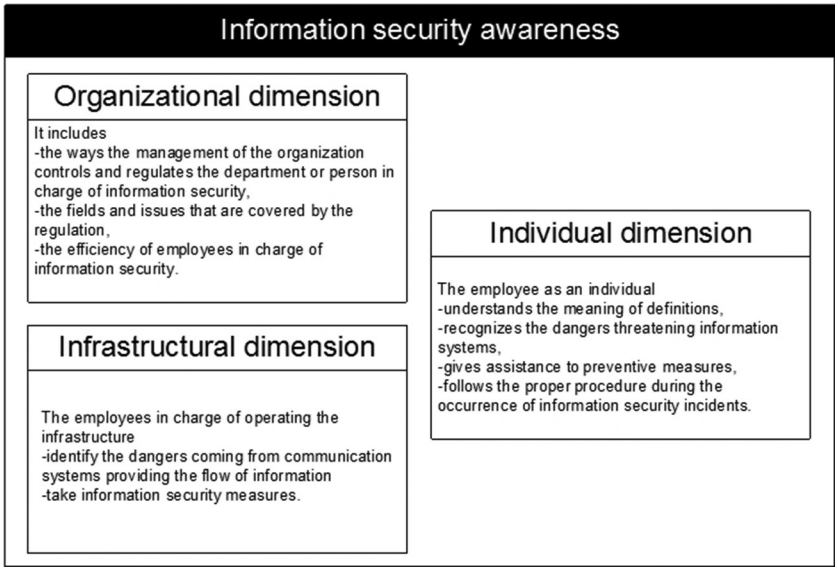



*Figure 1. The construct of ISA. [9]*

In Figure 1. we depicted the general model of ISA which in that form can serve as a measurement instrument about employees' perception on different dimensions of security.

In *organizational dimension* the following items can be tested:

- the ways the management of the organization controls and regulates the department or the concrete person in charge for 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) and internal factors (eg. regulations, the direct instructions of management, human resources management) have effects on organizational awareness. [10]

The *individual dimension* measures the IT knowledge, skills and abilities of the *employees*. Only those employees can make proper use of ICT who consciously apply information technology tools. 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.

Thirdly, *infrastructure dimension* covers partly communication (network) systems, devices and resources providing information flow between local information environments, and partly those organizational tools and resources which provide basic or value-added (information security etc.) services. [18] In view of the above, the infrastructural dimension 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.

Our model also suggests a normative approach to ISA; organizational, individual and infrastructural efforts should provide protection against *sources of danger* and to minimize risk causing breaches in information security. Sources of danger could be anything which results in a non-desired change in the function of one or more components of the information system. [17]

In order to classify employees into ISA categories we have used the Security Awareness Survey (SANS) questionnaire which was designed by information security experts in the US in 2012. [22] According to this the respondents are classified into five risk categories: [22] [9]

- employees belonging to the *first category* 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;
- *third category* represents the group of average risk, those employees, 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.

We intended to get further insight and verification of ISA by comparing ISA "categories" with employees' general ICT awareness which is described by their ICT literacy. For its general use in the literature, we used the concept of *digital literacy* which often overlaps with other similar notions (eg. information literacy, computer literacy), and can be applied as a suitable umbrella term. [14] Steve Covello identified more subareas and classified information literacy, media literacy, communication literacy, visual literacy and technology literacy as part of *digital literacy.* [4] He recommended five categories into which users can be classified:

- *excellent* if the 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.

During our research design we included measurement for *ISA* and for *digital literacy* constructs and classified employee responses into the appropriate categories both in the Austrian and Hungarian sample. In the following section we describe this part of the design and the characteristics of our two datasets.

## *Comparing Austrian and Hungarian Companies in ISA: Methodology and Sample Characteristics*

The analysis of the level of ISA in the Austrian and Hungarian business sector is at the centre of our research. Its primary purpose is to determine the conditions of information security awareness in both countries, in different size categories. We assume that the level of ISA in the business sector depends on:

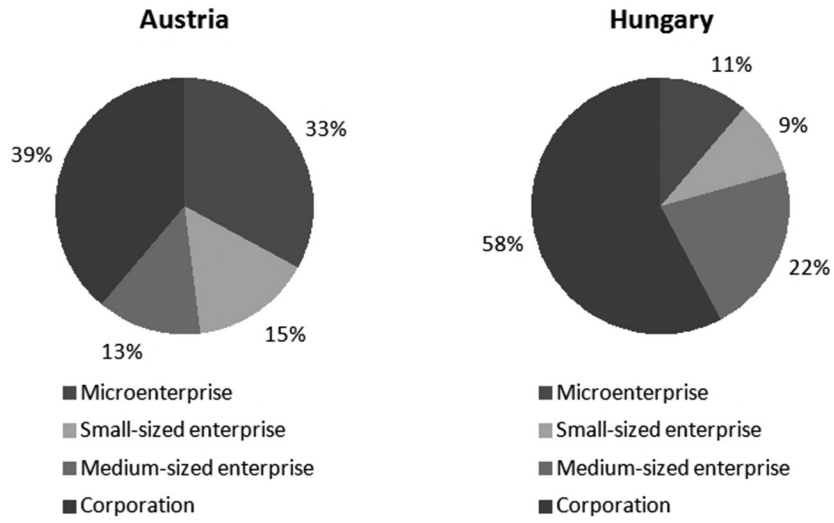
- company size and;
- the economic and information society development level of the country.

Our assumptions are based on the following research results: [21]

- a quarter of the Hungarian corporations still neglect IT audits;
- the strategic importance of information security has already been recognized by Hungarian corporations and enterprises but in terms of actual measures, they are still behind countries with a higher level of IT development such as Austria;
- in comparison to the international trends, the issue of information security is given less attention by Hungarian corporations and enterprises.

The classification of the parts of the *business sector* and of the size of enterprises in Hungary is determined by Act XXXIV of 2004 on The Small and Medium-Sized Enterprises and their Development. [1] The act defines the concepts of microenterprises, small and medium-sized enterprises as well as corporations.

The basis of our primary research was SANS which had already been developed and used. [22] The questionnaires were filled out both online and in a paper-based format with the help of the students at Karl Franzens University in Graz in Austria and at the University of Miskolc in Hungary, regardless of the demographic and employment data of the respondents. The questionnaire was filled out by 280 persons in Austria and 470 persons in Hungary until November of 2014. The number of respondents employed in the Austrian business sector was 152 persons and 116 persons in Hungary.




*Graph 1. The division of the respondents to the questionnaire on information security awareness in the Austrian and Hungarian business sector. [Source: own]*

Since we had no previous insights into the conditions of ISA in the business sectors either in Austria or in Hungary *exploratory research* was the suitable approach, and the analysis of the filled-out questionnaires was executed accordingly.

For comparative analysis we have to note that added value of corporate ICT use is very different in the two countries. [20] Added value at basic prices can be simply defined as the difference between gross output (at basic prices) and intermediate consumption (at purchaser prices) and can be decomposed into the following components:

- Compensation of Employees;
- Gross Operating Surplus;
- Mixed Income;
- Other Taxes on Production less Subsidies on Production. [20]

Compared to the EU average of 27 countries, the average added value of the Austrian enterprises was higher by 70% with EUR 530,000 in 2012. In contrast, the average data of the Hungarian enterprises did not exceed EUR 87,000 which was equal to only 27% of the EU average.

*Table 1. Average added value by size categories in Austria and Hungary in 2012. [20]*

| **Country /thousand EUR/** | **Micro-enterprise** | **Small-sized enterprise** | **Medium-sized enterprise** | **Corporation** | **Average** |
|---|---|---|---|---|---|
| EU27 | 71.56 | 880.52 | 5,250.82 | 61,900.78 | 311.77 |
| Austria | 124.19 | 1,042.24 | 7,640.42 | 64,716.60 | 530.42 |
| Hungary | 16.70 | 315.22 | 2,269.61 | 29 495.48 | 86.58 |

The added value of microenterprises in Austria reached 173% and a modest 23% in Hungary in relation to the EU average. It mounted up to only EUR 17,000 in Hungary and EUR 124,000 in Austria per enterprise, which was nearly 7.5 times higher than the Hungarian data in 2012. The added value created by small-sized enterprises was eight times higher in Austria (EUR 1,042,000) and 18 times higher (EUR 315,000) in Hungary compared to microenterprises. The added value generated by the Hungarian medium-sized enterprises was only slightly over 40% of the average of the European Union (EUR 2,270,000). In the meantime, the added value of the medium-sized enterprises in Austria exceeded the EU average by 45%. Regarding the performance of the Hungarian enterprises, the corporations operating in the country lagged behind their Austrian counterparts to the least extent. The added value per enterprise in Austria was three times higher in the case of small- and medium-sized enterprises and two times higher in the case of corporations compared to their peers in Hungary. [20]

We also see large differences in the state of the information society according to the EGDI (E-Government Development Index) measured by the UN. [23] EGDI has three components with equal weights: OSI (on-line service index), TII (Telecommunication Infrastructure Index) and HCI (Human Capital Index). Leading countries in the world according to most recent data are the Republic of Korea (1), Australia (2) and Singapore (3) and in Europe they are France (4), the Netherlands (5), the UK (8), and Finland (10).

*Table 2. Comparison of Hungary and Austria in EGDI ranking UNPAN, 2014. [23]*

| | EGDI | 2014 rank | 2012 rank | Change (2014–2012 | Category of EGDI |
|---|---|---|---|---|---|
| Hungary | 0,6637 | 39 | 31 | –8 | Middle |
| Austria | 0,7912 | 20 | 21 | +1 | Very High |
| EU Average | EGDI = 0,7300 | | | | |
| World Average | EGDI = 0,4712 | | | | |

In Table 2. we compared AT and HU in EGDI ranking and we can notice that both the actual position and category of the two countries (AT = 20, HU = 39) are different, but also the rate of development is more dynamic in AT then in HU (while AT has improved one place, Hungary has dropped eight between 2012 and 2014).

## *The Situation of ISA in Austria and Hungary*

Looking at the findings globally, it can be stated that in two categories (corporations and medium-sized enterprises) in our sample in Austria, the rate of organizations belonging to the safest category is more than 20%. Somewhat surprisingly, better results than that are shown by the corporations as well as the medium-sized enterprises in the Hungarian sample. The ratio in their case reaches and exceeds 30%. The findings of the second category, where the employees are aware of the possible dangers but they do not keep all the regulations, show a rather unified picture: three-quarters of the corporations, medium-sized and small-sized

enterprises in Austria belong to this category. As for the Hungarian small-sized enterprises, 100% of them fall into the second category and the same can be said about more than three-quarters of the microenterprises. A quarter of the Austrian small-sized enterprises, half of the microenterprises and three-quarters of the Hungarian microenterprises can be found in the third category where the employees definitely need further training on information technology. Moreover, there are some employees who are not aware of the dangers of information technology at 3% of the Austrian microenterprises.

*Table 3. The qualification of information security awareness among the Austrian and Hungarian enterprises. [Source: own]*

| Name | Austria | | | | | Hungary | | | |
|---|---|---|---|---|---|---|---|---|---|
| | First category | Second category | Third category | Fourth category | Fifth category | First category | Second category | Third category | Fourth category |
| Corporation | 20% | 77% | 2% | 0% | 0% | 31% | 61% | 8% | 0% |
| Medium-sized enterprise | 29% | 71% | 0% | 0% | 0% | 30% | 50% | 20% | 0% |
| Small-sized enterprise | 0% | 75% | 25% | 0% | 0% | 0% | 86% | 14% | 0% |
| Micro-enterprise | 8% | 43% | 48% | 0% | 3% | 0% | 59% | 33% | 8% |

Comparing ISA in the business sector in the two countries, it can be stated that Austria performs better in the size category of microenterprises and medium enterprises, while Hungary shows better results in the size categories of corporations and small-sized enterprises.

83% of the Austrian corporations said that they maintained *an IT security department*. High rates are achieved by the Austrian medium-sized enterprises (70%) as well. The highest rates, however, are shown by the Hungarian corporations with 90%. They are followed by the medium-sized enterprises employing less than 250 people (84%), then the small-sized enterprises (36%). The lowest rates are produced by the Hungarian (30%) and Austrian (14%) microenterprises with low levels of capital and human resources.

In terms of the *organizational dimension*, only the Hungarian corporations produce good results, appearing in the top two risk categories.

*Table 4. The qualification of information security awareness in the Austrian and Hungarian business sector based on the organizational dimension. [Source: own]*

| Name | Austria | | | | | Hungary | | | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | First category | Second category | Third category | Fourth category | Fifth category | First category | Second category | Third category | Fourth category | Fifth category |
| Corporation | 4% | 71% | 25% | 0% | 0% | 17% | 72% | 11% | 0% | 0% |
| Medium-sized enterprise | 0% | 47% | 53% | 0% | 0% | 17% | 44% | 30% | 9% | 0% |
| Small-sized enterprise | 0% | 29% | 52% | 19% | 0% | 0% | 25% | 75% | 0% | 0% |
| Micro-enterprise | 0% | 14% | 43% | 36% | 7% | 0% | 25% | 42% | 25% | 8% |

It was surprising to see that a quarter of the Austrian corporations fell into the third risk category. Furthermore, nearly a fifth of the Austrian small-sized enterprises and more than a third of the microenterprises pose a serious threat in terms of security. The same can be said about a quarter of the Hungarian microenterprises. In addition, 7% of the Austrian microenterprises fall only into the fifth category.

It is important to examine in each department *whether there is a regulation on the use of IT tools* or if they apply general rules that also include the use of IT tools. A third of the respondents in Austria and a quarter of them in Hungary could not say whether there were such policies in their workplace. This rate reaches 46% in the case of the Austrian small-sized enterprises. Nearly half of the Austrian microenterprises and more than 80% of their Hungarian counterparts reported that they did not apply any regulations relating to information technology. On the other hand, half of the Austrian corporations and two-thirds of their Hungarian peers used specific IT regulations and guidelines. It can also be said about a third of the Austrian medium-sized enterprises that a quarter of them had IT-related issues within their general regulations. Half of the medium-sized enterprises in Hungary also included their IT rules into their general regulations. In the size category of small-sized enterprises, 40% of them in Hungary and a quarter of them in Austria had some sort of written regulation on the use of IT devices.

Two-thirds of the employees at the Hungarian enterprises were satisfied with the standard of the *training* they received on information security, contrary to this, the same rate was only 28% in their Austrian counterparts in 2014. The rate of employees satisfied with the training on information security reached 40% in the category of microenterprises and small-sized enterprises, 60% in the medium-sized enterprises and 70% in the corporations in Hungary. As for the Austrian business sector, worse rates were measured. Nearly a third of the respondents in the Austrian microenterprises, small and medium-sized enterprises reported that they received appropriate training on information security. A fifth of the employees at Austrian corporations reported the same.

Another part of the organizational dimension is the examination of *access to certain websites* and their regulation at the workplace. In general, it can be said that more than 80% of the corporations in Austria and more than 90% of them in Hungary regulated accessible content

on the Internet while the same rate was 20% at microenterprises in both countries. Nearly 40% of the small-sized enterprises in Austria and 55% of the medium-sized enterprises had such policies. 30% of the small-sized enterprises in Hungary and 35% of the medium-sized enterprises had regulations on the accessibility of certain websites and they were kept by the employees. It is surprising that employees did not keep the regulations at a fifth of the corporations in both countries.

A further part of the organizational dimension is *the regulation of mail delivery systems*. In this case it is also true that the rate of regulation increases together with the size of the organization – both in the number of employees and in terms of asset value. There are regulations on the use of mail delivery systems at 70% of the Austrian corporations and three-quarters of the Hungarian corporations. In contrast, only 10% of the microenterprises in Austria and Hungary regulated the use of mail systems by their employees. Nearly half of the small and medium-sized enterprises both in Austria and Hungary did not regulate the use of mail systems.

The idea behind *the emergence of cloud computing* is that information procession is much more efficient if it is done through centrally coordinated computer data storage systems accessible through a network. It is also a part of the *organizational dimension*. The term "cloud" is derived from the representation of the Internet network diagrams and is used to indicate the unknown or irrelevant parts of a system. Nearly 45% of the respondents in the Hungarian business sector – and 30% in Austria – did not know whether the use of cloud computing services is regulated at their workplace. Corporations both in Austria and Hungary either did not allow at all or only to a small degree permitted the use of cloud computing. A quarter of the Hungarian microenterprises and 55% of their counterparts in Austria said that they were authorized to use such applications as Dropbox and Google Drive for storing institutional or business data. At half of the small-sized enterprises in Hungary and at a third of their peers in Austria, the use of cloud computing is forbidden. The lowest rate of use was measured in the category of medium-sized enterprises in Hungary with 16%. The same rate did not exceed 10% among the corporations in Austria.

When examining *the individual dimension*, basically the general IT knowledge of the respondents is measured. It largely depends on the practice the employees had earned in previous years as well. The respondents mentioned an average duration of 16 to 18 years in Austria and 15 to 17 years in Hungary with regard to the use of computers. In terms of using the Internet, however, the average duration mentioned by the employees was an average of 12 and 14 years in Austria and 10 to 13 years in Hungary. If the daily use of computers is examined, we can conclude that the employees working in every company size category spend between 6 and 8 hours a day in front of the computer on average in both countries. From this, it can be concluded that, regardless of the size of their company, the respondents in the sample have similar practice and experience in this field.

Based on the individual dimension, the response rate in the first categories exceeded 50% in the case of the Austrian and Hungarian corporations and medium-sized enterprises, which is very favorable. Still, it is a bit alarming that 5% of the employees working at corporations in Hungary and 2% of them working in Austria were not aware of the dangers and safety principles.

*Table 5. The qualification of information security awareness in the Austrian and Hungarian business sector business and public sector based on the individual dimension in 2014. [Source: own]*

| Name | Austria | | | | | Hungary | | | |
|---|---|---|---|---|---|---|---|---|---|
| | First category | Second category | Third category | Fourth category | Fifth category | First category | Second category | Third category | Fourth category |
| Corporation | 62% | 16% | 20% | 2% | 0% | 54% | 29% | 12% | 5% |
| Medium-sized enterprise | 72% | 6% | 22% | 0% | 0% | 50% | 36% | 9% | 5% |
| Small-sized enterprise | 24% | 52% | 24% | 0% | 0% | 0% | 78% | 22% | 0% |
| Micro-enterprise | 28% | 43% | 26% | 2% | 2% | 0% | 75% | 17% | 8% |

It was an even bigger problem for microenterprises in Austria where 2% of the respondents fell into the fifth category, although at a quarter of the Austrian microenterprises and small-sized enterprises, there were responses falling into the first category. It can be seen from this, that the results were better in Austria in every size category from the perspective of data security.

As another interesting *part of the individual dimension*, it was also asked if the employees *noticed when their workstations were hacked into*. Hacking into a computer or computer system occurs when someone unlawfully enters or, by violating their scope of authorization, stays in the system by either breaching or circumventing its protection. More than 80% of the employees working in corporations in Hungary thought that they were able to notice when their workstations had been hacked into. In contrast, only a quarter of their peers in the Hungarian small-sized enterprises thought the same. In the case of the other examined Austrian and Hungarian organizations, a rate of nearly 60% could be observed.

Another important element in the framework of the individual dimension was the proportion of employees *voluntarily granting their company passwords* to other users. Respondents from the Austrian small-sized enterprises (40%) and the Hungarian medium-sized enterprises gave their company passwords to other users in the largest rate (40%). In contrast, employees working in the Hungarian small-sized enterprises were the most reluctant to give their company passwords to others (10%). At a quarter of the remaining Austrian organizations the practice of granting company passwords voluntarily also occurred.

A corresponding question to the previous one was whether *the respondent's boss had ever asked for their company password* or not. Surprisingly, such a case has already occurred at almost half of the Austrian small-sized enterprises. The same can be said about nearly a quarter of the corporations in Austria. A low prevalence, around 15%, was experienced in the case of the Austrian and Hungarian microenterprises, and the Hungarian medium-sized enterprises and corporations. The rates were measured between 20 and 25% in the remaining surveyed size categories.

Time and again, rumours start spreading about renowned portals being hacked into and unauthorized access to the passwords of hundreds of thousands or even millions of users coming to light. In reality, it represents a serious security risk if many people use *the same*

*password* everywhere. Within the context of the individual dimensions, we examined how cautious the respondents were in this regard. 15% of the respondents in Austria and a tenth of them in Hungary stated that they *used the same password* at work and in their private life as well. 15% of the Hungarian microenterprises and a quarter of their Austrian peers did not use the same password while there were just a few people at the Hungarian small-sized enterprises and the Austrian corporations (9%) who used their private password in their workplace.

If we look at the organizations where *there are rules to change passwords and whether they actually change them*, it can be stated that half of the Austrian microenterprises and small-sized enterprises as well as two-thirds of the Hungarian medium-sized enterprises did not have any rules or regulations to change passwords and they did not actually change them. In contrast, almost 90% of the Austrian and Hungarian corporations introduced certain regulations for changing passwords and their employees actually kept those rules sometimes even without having any regulation on the change of passwords.

The illegal *installation and use of software (software piracy)* as well as downloading files for personal use also has to be examined within the concept of the individual dimension. Software piracy and downloading files for personal use were typical of three-quarters of the Hungarian microenterprises, a quarter of the medium-sized enterprises and 60% of the small-sized enterprises in 2014. In Austria, these rates were lower, half of the microenterprises, a third of the small-sized enterprises and a tenth of the corporations reported that their employees downloaded files for personal use.

In the responses given to a number of questions related to the *infrastructural dimension*, a lack of knowledge or the overvaluation of some infrastructural parts appears quite frequently. Such a statement can be the one according to which the information stored in the employee's computer is of no value for 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. In contrast, the same rate was only 10% in Austria in 2014. A fifth of the Austrian micro and small-sized enterprises, and less than 5% of the medium-sized enterprises and corporations thought that they were not a target of this type of attack. In Hungary, nearly half of the micro and small-sized enterprises, a third of the medium-sized enterprises and 36% of the corporations thought the same.

In Austria, corporations achieved the best ratings in the *infrastructural dimension of ISA* with a rate of nearly 60%. Even the Hungarian corporations could reach a good rate of responses, falling into the first category by reaching 37%. However, in the case of the Hungarian medium-sized enterprises, due to a fifth of their employees' responses, the classification into the third category means that they would need further training. The same rate was 5% for the Hungarian corporations and 13% for the Austrian microenterprises.

*Table 6. The qualification of information security awareness in the Austrian and Hungarian business sector based on the infrastructural dimension. [Source: own]*

| Name | Austria | | | Hungary | | | |
|---|---|---|---|---|---|---|---|
| | First category | Second category | Third category | First category | Second category | Third category | Fourth category |
| Corporation | 58% | 42% | 0% | 37% | 57% | 5% | 2% |
| Medium-sized enterprise | 45% | 55% | 0% | 29% | 52% | 19% | 0% |
| Small-sized enterprise | 30% | 70% | 0% | 11% | 56% | 11% | 22% |
| Micro-enterprise | 35% | 52% | 13% | 17% | 75% | 8% | 0% |

As part of the *infrastructural dimension*, the availability of *installed, updated and licensed antivirus programs* was also examined. More than 90% of the employees working in the surveyed Austrian and Hungarian organizations said that they had antivirus software installed on their computer.

Another question we sought to answer was whether *the employees found a virus on their computers*. A computer virus is a program that hides its own copies in other executable programs or documents. It is mostly malicious, having the capability of making other files useless or even completely destroying them. Nearly a fifth of respondents claimed to have encountered a computer virus during their work. A higher proportion was found in the case of the Austrian microenterprises (46%) and small-sized enterprises (22%), and the Hungarian small-sized (45%) and medium-sized enterprises (36%). The lowest rate was found in the Austrian corporations public institutions (6%). Nearly 8% of the employees working in the Hungarian microenterprises could not say if they had ever found such undesired programs on their computers.

Within the framework of *the infrastructural dimension*, the *frequency of automatic updates* was also examined in the business and the public sector. Nearly 70% of the surveyed Hungarian organizations and 60% of the Austrian organizations used the function of automatic updates. 6% of the Hungarian corporations, a tenth of the small-sized enterprises, 12% of the Austrian microenterprises, 9% of the small-sized enterprises and 20% of the medium-sized enterprises working in local governments and 40% of them working in other local government organizations could not tell whether there was an automatic update function on their own computers at work.

It can be concluded that a close relationship can be observed between the information security awareness and the digital literacy of employees. As for Hungary, each respondent having poor or bad digital literacy fell into the third risk category. Based on the responses, 40% of the employees with poor IT skills fell into the third one, while 60% of them fell into the second risk category. More than threequarters of the employees relying on some assistance to recognize their IT needs fell into the second risk category, a fifth of them fell into the third, and only 8% of them could be classified in the first category. Surprisingly, employees with good and excellent IT skills were mainly found in the second category in the largest number. Only 7% of employees having good digital literacy could fall into the first risk category while a third of them were in the third one. Sadly, less than a fifth of the employees with excellent IT skills fell into the third risk category in terms of information security in Hungary.

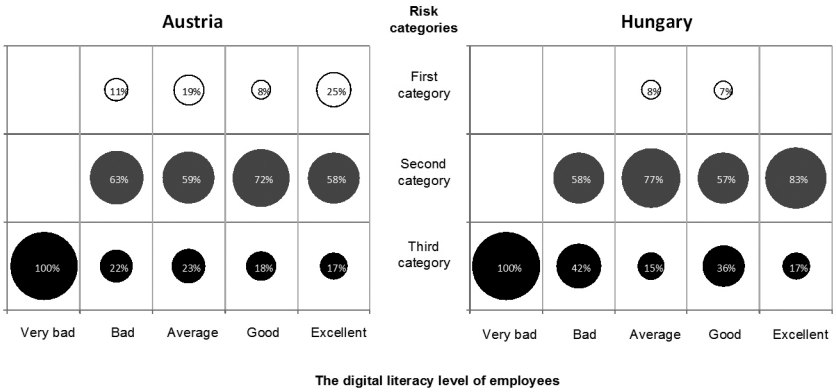



*Figure 2. The connection between global risk categories and the digital literacy of employees in Austria and Hungary. [Source: own]*

A quarter of employees having excellent digital literacy in Austria can be found in the first, the remaining 60% of them fall into the second category of global information security awareness. A tenth of those who have good digital literacy belong to the first category, three-quarters of them fall into the second but 18% of them get into only the third category. A fifth of the employees in bad need of some assistance in information technology have excellent, 59% of them good, and a quarter of them average digital literacy in terms of information security awareness. Each of the employees having bad digital literacy fall into the third risk category.

## Conclusions

In our study, we reviewed the conditions of information security awareness in the Austrian and Hungarian business sector as well as their positions relative to one another.

It is true about both countries that the level of information security awareness is lower in the case of enterprises belonging to smaller size categories, when compared to the larger ones. IT regulations and training on information security are more frequent, accessibility to certain websites and the use of mail delivery systems are regulated, and password changes are required at corporations. In the case of micro and small-sized enterprises, it is hardly possible to find an organization or person that is entitled to deal with information security issues, regulations on IT are mostly missing, and they rarely participate in training in information technology. Access to certain websites and the use of mail delivery systems are also rarely regulated. Because of the lack of training, considerably fewer employees know about cloud computing in the enterprises employing less than 50 people in comparison to their counterparts working in bigger enterprises. It is also typical of the microenterprises that their employees are less likely to give their passwords whether they are forced to do so or not. When comparing the two countries by size categories, differences can hardly be found in terms of information security awareness.

As for the organizational dimension, the Hungarian enterprises performed better in all size categories. It can be traced back to a lower level of regulation and a more critical attitude towards training shown by the employees in Austria. A good level of information security

awareness was observed among the Austrian medium-sized enterprises with less than 250 employees, however, in a fifth of their Hungarian counterparts, the employees need further trainings in this area. Security problems can be traced back to poor organization at a fifth of the Austrian small-sized enterprises, a third of the Austrian microenterprises, and three-quarters of the Hungarian microenterprises.

In terms of the individual dimension, the Austrian enterprises came up with better results in every size category. Password changes are more frequent and the practice of illegal installation and software use occurs less often. Employees working in a fifth of the Austrian and Hungarian enterprises have distressing gaps in their knowledge in this area.

As far as the infrastructural dimension is concerned, the Austrian small and medium-sized enterprises outperformed their Hungarian peers in every size category. Furthermore, it can also be concluded that employees with higher digital literacy have a higher level of information security awareness in a surveyed country, and the rate of employees with excellent digital literacy is also higher than it was measured in Hungary, resulting in a more favorable level of information security awareness compared to the Hungarian business sector.

## References

[1] *Act XXXIV of 2004 on the Small and Medium-Sized Enterprises and their Development*.

[2] CHANG, L., JACK, T., MARCHEWKAB, J., JUNE, L., CHUN-SHENG, Y.: Beyond Concerns: A Privacy-Trust-Behavior Intention Model. *Information & Management (I&M)*, 42 1 (2005), 289–304.

[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.

[4] COVELLO, S.: *A review of digital literacy assessment instruments*. Syracuse: Syracuse University, School of Education. Analysis for Human Performance Technology Decisions, 2010.

[5] DESMAN, M. B.: The Ten Commandments of Information Security Awareness Training. *Information Systems Security*, January/February (2003), 39–44.

[6] GORDON, A. L., MARTIN, P. L., LUCYSHYN, W., RICHARDSON, R.: 2006 CSI/FBI Computer Crime and Security Survey. *Computer Security Institute*, 2006.

[7] HAIG Zs.: Az információbiztonság komplex értelmezése. (A Complex Interpretation of Information Security). *Hadmérnök*, Különszám online, (2006).

[8] HAIG Zs., KOVÁCS L.: Fenyegetések a cybertérből. (Threats from Cyberspace). *Védelempolitika*, 61–69. www.nemzetesbiztonsag.hu/letoltes.php?letolt=57 (downloaded: 02 01 2015)

[9] ILLESSY M., NEMESLAKI A., SOM Z.: Elektronikus információbiztonság-tudatosság a magyar közigazgatásban. (Information Security Awareness in the Hungarian Public Administration). *Információs Társadalom*, 14 1 (2014), 52–73.

[10] KODAJ K.: A Nemzeti Elektronikus Információbiztonsági Hatóság. (Introduction to the National Electronic Information Security Bureau). 2013, 1–19. www.kifu.gov.hu/kifu/sites/default/files/NFM_Ibtv_NEIH_2013_12_18.pdf (downloaded: 02 01 2015)

[11] KOVÁCS L.: Az e-közszolgálatfejlesztés nemzetbiztonsági és hadtudományi kérdései. (National security and military aspects of e-government development). In. NEMESLAKI A.: *E-közszolgálatfejlesztés. (E-public service development).* Budapest: NKE, 2014, 227–248.

[12] KOVÁCS L., KRASZNAY Cs.: Digtális Mohács – Egy kibertámadási forgatókönyv Magyarország ellen. (Digital "Mohács" – A possible scenario of a cyberattack against Hungary). *Nemzet és Biztonság*, 2 (2010), 44–56.

[13] KÜRT Zrt.: *Informatikai biztonsági tudatosság oktatása. (The Education of Information Security Awareness).* www.kurt.hu/megoldasaink/informatikai-biztonsagi-tudatossag-oktatasa/ (downloaded: 02 01 2015)

[14] LÉVAI D.: A digitális állampolgárság és digitális műveltség kompetenciája a pedagógus tevékenységéhez kapcsolódóan. (The Competence of Digital Citizenship and Digital Literacy In Relation To Pedagogical Activities). *Oktatás-Informatika*, 1–2 (2013), 1–7.

[15] MARK, B. D.: The Ten Commandments of Information Security Awareness Training. *Information Systems Security*, January/February (2003), 39–44.

[16] MUHA L.: Az informatikai biztonság egy lehetséges rendszertana. (Recommendation for a framework for information security). *Bolyai Szemle*, 17 (2008), 137–156.

[17] MUHA L.: Fogalmak és definíciók. (Terminologies and Definitions). In. MUHA L. (szerk.), *Az informatikai biztonság kézikönyve: Informatikai biztonsági tanácsadó A-tól Z-ig. (The Handbook of Information Security – Information Security Guidance from A to Z).* Budapest: Verlag Dashöfer, 2004, 1–37.

[18] MUNK S.: Információs színtér, információs környezet, információs infrastruktúra. (Theater of Information, Information Environment and Infrastructure). *Nemzetvédelmi Egyetemi Közlemények*, 2 (2002), ludita.uni-nke.hu/repozitorium/bitstream/handle/11410/1083/nek_2002_2_munk.pdf?sequence=1 (downloaded: 02 01 2015)

[19] PÓSERNÉ O. V.: Az információs társadalom és a terrorizmus kapcsolata. (The Relationship between the Information Society and Terrorism). *Bolyai Szemle*, 1 (2006), 145–159.

[20] SASVÁRI P., RAUCH, W.: Information Systems and Economic Value Added: A Comparative Illustration of Austria and Hungary. In. NEMESLAKI (Ed.), *ICT Driven Public Service Innovation*. Budapest: National University of Public Service, 2014, 51–72.

[21] SZABOLCS A.: *Információbiztonsági helyzetkép 2011. (A Snapshot on Information Security, 2011).* ISACA Magyarországi Egyesület, 2011.

[21] TRENTON, B., CORTNEY, S., DAVE, P.: *Security Awareness Survey, 2012*. www.securingthehuman.org%2Fmedia%2Fresources%2Fplanning%2FStage03-03-HumanRiskSurvey.docx&ei=lCj7VNPCC4HnUPrRgZAH&usg=AFQjCNHWvTu4TL_ttLlGaCMk3UDFAUEYqw&bvm=bv.87611401,d.d24&cad=rja (downloaded: 02 01 2015)

[23] UNPAN: *United Nations E-Government Survey 2014: E-Government for the Future we Want.* New York: United Nations Department of Economic and Social Affairs, 2014.