UNIVERSITY OF PUBLIC SERVICE
Doctoral School of Public Administration Sciences

Zoltán Som

# Issues of Information Security Awareness in Public Administration

Doctoral (PhD) Dissertation

## THESIS BOOKLET

Supervisor:
Dr. Tamás Szádeczky, associate professor

2021, Budapest

# 1 THEME AND OBJECTIVES OF THE DISSERTATION

In our accelerated world, the volume of knowledge is constantly increasing, more and more complex knowledge is needed for the operation, use and security of IT systems. Lifelong Learning (LLL) has become a basic requirement. Instead of lexical, theoretical knowledge, adaptive and innovative skills of individuals should be developed due to the excessive dynamism of the knowledge-driven economy and society as well as the working environment. The ability and desire to learn independently allows for successful adaptation to an ever-changing environment and personal renewal. One of the reasons for the success of well-performing organizations is that leadership and organizational development are part of the organizational strategy. An investment that ensures long-term efficiency and the effective functioning of the organization. The learning education challenge has become complex (continuous lack of time, stress, multitasking, continuous change, etc.), which cannot be effectively addressed with the help of traditional forms of training. Labor organizations and employees need support that is individually about them as far as possible, is time-saving, practical yet enables continuous, independent self-improvement. This requires a combination of novel teaching methods. In addition to formal education, it is necessary to include additional channels to transfer knowledge and raise awareness. Information security challenges require, in parallel, that the organization has the ability to react to current, rapidly changing risks and attack vectors as one person. In my dissertation, I present the development of the regulatory environment in Hungary relevant to information security from 1994 to the recent past. Act L of 2013 (on the electronic information security of state and local government bodies) was adopted by the Parliament on 15 April 2013, and was published on 25 April 2013. Later that year, the education of the Electronic Information Security Manager (abbreviated in Hungarian as EIV) specialization started at the National University of Public Service (official Hungarian abbreviation: NKE) as a vocational training program, with which the university-level training of Hungarian information security managers was launched. In fact, this part of the law, as well as the launch of the training of professionals, is an extremely important step and is considered to be symbolic: it draws attention to the importance of education. The appropriate level of information security is clearly important not only for the individuals or for the labor organizations, but it is also a national interest and it is also important in an economic perspective. However, this cannot be achieved without the training of adequately qualified professionals. Information security awareness and preparedness are important both in terms of private interests and from a public point of view in terms of customer confidence and trust in information systems and electronic public services. In addition to public administration, e-administration should also be mentioned, which has been developing and spreading for years, i.e. its use is becoming more and more widespread both in public administration and on the user side, with citizens. According to Budai (2016): "The development of e-administration is a constraint dictated by the successive (social, technological, political, legal, etc.) components of the information society." It thus affects both those working in public administration and practically all citizens at a national level using administrative services; and later its possible connection with European Union processes may appear, or we may think about other international administrative relations, activities at both state and international levels. This, in turn, requires not only administrative developments (strictly speaking), but also the development of competencies and knowledge. Budai (2016) puts it this way: "As surprising as it is, modernization of public administration on the user side begins with the development of essential competencies: literacy education, which is increasingly moving toward the dimensions of digital literacy. Additional competencies provide the opportunity for independent development and lifelong learning. Users therefore need to be trained and their programs (…) shall be adapted to the scheduled renewal of public administration. At the same time, programs that support the more efficient use of public services by citizens need to be strengthened. These include: business assistance and IT mentoring." Education (in the field of information security) may require the assessment and development of existing and required IT competencies. (Bujdosó, 2014) Furthermore, it should be taken into account that proficiency in the use of the transmission medium can also significantly influence the utilization of the knowledge and information to be transferred. (Bujdosó, 2015)

It is also clear that the development of information security competencies is also essential where the user side extends beyond those working in public administration; and it is also necessary to think about those who use administrative services (the citizens for example). In addition to all these e-administrative and administrative aspects related to the state, the ICT sector, which is significantly present in regards of GDP, and e-trade developments and investments should be mentioned as well. (Som, Papp 2015)

Based on Act L of 2013, followed by the implementing regulation of the Ministry of the Interior (41/2015 BM) and the sector-specific [17/2019. (VIII. 15.) BM instruction; [on the Issuance of the Code of Conduct for Security-Awareness of Electronic Information Security of the Bodies Managed by the Ministry of the Interior and the Minister of the Interior], there is a clear need (at regulation level) for information security training in order to achieve development on this field. These processes started already in 1994 with recommendation No. 8 of the

Interdepartmental Committee on Informatics titled: IT Security Methodology Manual. This was followed in time by recommendation No. 12 of the Interdepartmental Committee on Informatics in 1996, titled: Security Requirements for IT Systems. In 2008, Recommendation No. 25 of the Administrative Informatics Committee, titled: Hungarian Information Security Recommendations (Hungarian abbreviation: MIBA) was issued, which is in fact a collection of recommendations. As well as other important legislation specific to the sector, affecting information security. I. e. the requirement for privacy certification is set out in Section 100 (1b) of Act XL of 2008. (on Natural Gas Supply) and in Section 63 of Act CCIX of 2011 (on Public Water Utility Services). Furthermore, with the Strategy on the Security of Network and Information Systems in Hungary [Ministry Decree no. 1838/2018. (XII. 28.)], the legislative intention may be linked to the creation of a competitive domestic knowledge base for cyber security education, training and research and development opportunities. Regarding the regulation, the Hungarian public administration has been brought to the forefront by Act L of 2013, as it created a good basis for information security efforts, however, during the processing of the literature, I came to the conclusion that many authors also included different HUMAN aspects in their research. REGULATION (as in law-making) is present among the factors I have examined as a so called HARD requirement, while I have taken into account the newly published HUMAN factors as SOFT factors with which to increase the efficiency of information security. I present this system of correlation, i.e. the main line of my research, in Figure 1 below.

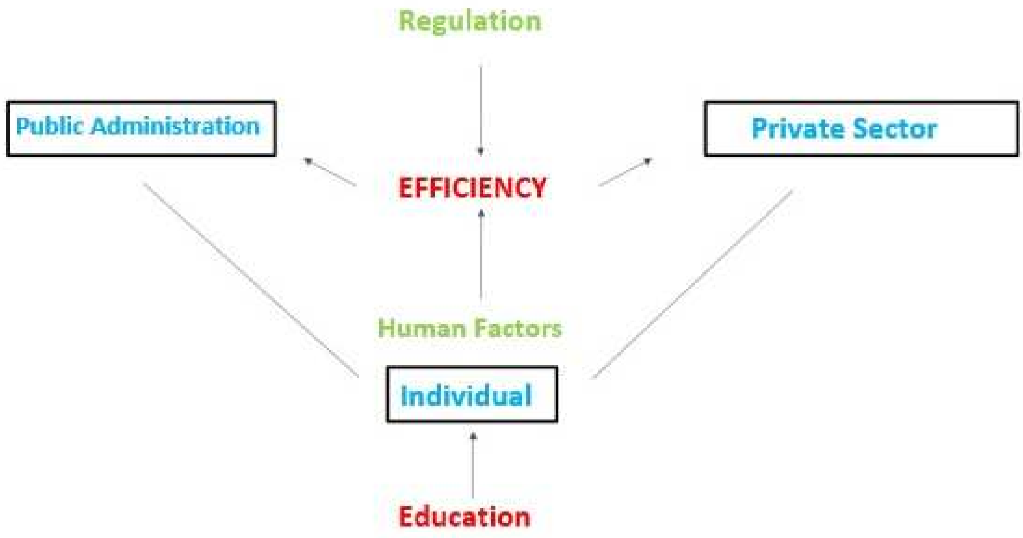

Figure 1: System of Correlation Regarding the Research

It can be seen from the figure above that the effectiveness of information security can be increased by increasing the efficiency of a sphere through the awareness of the individual, which can be achieved through education. Education serves the purpose that if the individual understands it more effectively, he/she will accept and even follow the policy more effectively as well, i.e. he/she will make information security even more effective. PUBLIC ADMINISTRATION has an extremely important role (and responsibility) in this respect, as the public administration is a set of organizations that perform public tasks, provide services and act in matters of national importance. And if we consider the set of organizations making up the system of public administration as one of the largest employers in Hungary, changes on a national level can be induced by improving the knowledge of those who work there.

Critical areas of information security development can be identified through baseline measurement and evaluation followed by training (based on the outcomes) and evaluation thereof. In fact, measuring the current level (the so-called ‘As Is’ state) is important so that the changes can be measured and monitored afterwards. In recent years, it can be seen that we have not achieved the state yet to present those responsible for administrative information security the necessary tools in an organized way, or to start such a process in a self-organized way. There are several initiatives to enable these information security officers to build professional relationships with each other or with market players, but their purpose and function are different. It can therefore be stated that the information (information security recommendations presented above) and legal conditions are given. That is why I set out to study this in order to examine the facts in an objective way, to resolve the apparent contradiction that emerged from a sample of a small group in a work organization, or from feedback received during education. However, differences have already emerged in the following areas: how organizations have been able to apply this information, how they have interpreted recommendations and legislation, what they mean by education, and how effective compliance has been as a result. In my dissertation, I have examined only specific issues related to information security education. This characteristic of some organizations was not examined, e.g. how the recommendations and legislation were interpreted, or how they were incorporated into the processes.

From the point of view of the Hungarian public administration, the dissertation can be linked to the following objectives:

- Hungary’s Strategy on the Security of Network and Information Systems [Ministry Decree no. 1838/2018. (XII. 28.)], can be linked to cyber security education, training and research and development opportunities as well as the creation of a competitive domestic knowledge base.

- Hungary’s Digital Education Strategy sets out goals and measures for the development of digital competencies, awareness and information, and education and vocational training areas that promote information security, with the same impetus.
- In addition, Section 1 of Chapter I of Act L of 2013 classifies it as an administrative protection measure in connection with the provision of NKE training activities in Chapter IV, at the part on Education and Training;
- and Article 3.1.7 of the BM Implementing Decree no. 41/2015 in the Chapter on Awareness and Training, also it is listed as mandatory from Security Class 1 and onwards.

# 2 OBJECTIVES, HYPOTHESES AND METHODS OF THE RESEARCH

The aim of my dissertation is to examine objective research data in the surveyed time interval. My aim is to gain momentum through my proposed solutions by identifying and removing the obstacles that hinder development which may occur in some work organizations. This way, following the level of administrative information security, as one of the important components, the level of national cyber awareness could start to increase significantly and measurably. In addition, although the recommendation in 1996 and subsequent collections of recommendations address the responsibility for the organization of education, this was later raised in Act L of 2013 and its Implementing Decree 41/2015 to a legal level. However, the implementation of this may vary from work organization to work organization. There is no requirement to perform pre-education (baseline, current) and post-education (understanding, awareness, compliance, changes) assessments and as a result there is no information available at national or administrative level. The assessments made in each administrative organization thus remain isolated and not comparable. However, as the collection of recommendations has been available to the entire public administration since 1996 and has been mandatory since 2013, it can be assumed that there is no lag or fallback in terms of information security awareness and regulation. After studying all these antecedents and following the international literature review, I examined and presented the factors influencing the behavior of the human (soft) factors and the regulation as the hard factor in connection with my hypotheses.

In order to meet the research goals, I formulated my hypotheses as the basis of my research as follows:

H1: There is no lag whatsoever in the Hungarian public administration sector in terms of the level of information security awareness compared to the Hungarian business sector.

H2: The practice of applying information security rules can be developed more effectively in the framework of attendance-based training compared to written regulations.

H3: The practice of applying information security rules can be developed within the framework of e-learning education.

In my dissertation I limited myself to presenting the information security trainings and qualifications available in Hungary and only examined the Hungarian public administration and the Hungarian business sector. The reasons for this are mostly length constraints, the time and cost constraints of foreign sampling and surveys, as well as the fact that my educational experience so far is with Hungarian organizations. Furthermore, the qualifications required of professionals by Act L of 2013 also apply to Hungary, so a deeper examination of other international qualifications or training is not relevant. The range of interpretation of the 7 researches presented in my dissertation differs from research to research, but it should be emphasized that in each case it contains only the answers of the employees working for the given organizations, and not the answers of each and every employee. In other words, there may be variations within the public administration sector, within or between organizations, but the sample size still allows us to draw conclusions, bearing in mind of course that there may be outliers.

In my research, I considered password management and its practices as one of the indicators of information security awareness and the ability to follow rules. Within the 3 main question blocks, the questionnaire asked for different answers to 72 questions. In the evaluation, I created an index of one group of scaled response options. Eight variables were equally weighted in the password management-information security awareness index, and in one case I transposed the values of the obtained answers, since the statement (I rarely change my password) had a negative logical quality and disagreement was the expected attitude from an information security point of view. I created an index from these eight variables, or rather from their evaluation. As a result, I obtained an average value of 4.33 for the public sector and a slightly higher average value of 4.38 for the aggregate index value for the business sector. In this context, it is important to point out that, as it is an aggregate index, this discrepancy is extraordinary and demonstrates that public administration is lagging behind in this respect.

To make a more complex comparison between business and public administration, I have carried out statistical tests. I used the IBM SPSS statistical software package to process the incoming data. The statistical tests showed significant differences between the responses of business and public sector employees.

In my second hypothesis, I examined the question of whether the practice of information security rule application can be more effectively developed through “live” education (that required actual attendance) or through written regulation, using the number of reporting incidents as an indicator.

In order to support my hypothesis, I had the opportunity to examine two separate work organizations, i.e. I had the values before and after the publication of the Information Security Regulations (Hungarian abbreviation: IBSZ) and the Information Security Policy (Hungarian abbreviation: IBP), broken down by month. These intervals, i.e. the values before and after the publication of the information security policy and the trends before and after the attendance training, showed significant differences according to the statistical tests carried out.

In an e-learning solution, the SCORM (Sharable Content Object Reference Model) can be imported into a standard package so that it can be played in any LMS (Learning Management System). In this study, I used Moodle (LMS) as it was available in the company. The e-learning courses used the facilities provided by the Moodle system, but there was no involvement of tutors or other human resources, so only electronic content was available to the participants. The e-learning courses were advertised as intranet news, not as compulsory course material. (The regulations and policies were published in a similar manner.) An important point is that the use of e-learning systems also requires pre-existing ICT skills, so it is necessary to assess and support their use (Bujdosó 2014).

For the E-mail Security Fundamentals e-learning course, a pass mark of 80% was required in order to pass the test. Of the 2,853 attempts to complete the test, 2,196 belonged to unique individuals. The questionnaire, published in conjunction with but separate from the e-learning course, was completed by 902 individual respondents, who rated the training on a five-point scale and indicated why they found it useful. The test for the e-learning course titled “Password Security at Beginner Level” was taken by 1,976 unique respondents, with 2,902 attempts all together. A 75% pass mark was required in order to pass the test. The questionnaire, which was published separately from but linked to the e-learning course, was completed by 901 individual respondents, who rated the course on a five-point scale and indicated why they found it useful. The test for the e-learning course titled “How to defend against phishing attacks” was started by 2,667 unique respondents, with 3,454 attempts all together. A pass mark of 70% was required in order to pass the test.

I examined the periods before and after the publication of the information security policy as well as the periods before and after the e-learning materials were published and the correlation with the number of user notifications.

The research presented in my dissertation is not an assessment of the public administration as a whole, nor of all its employees, i.e. it cannot be considered a representative sample. Nevertheless, a valid conclusion can be drawn from the study for those who completed the questionnaire and for a given point in time, an approximately good and accurate picture can be obtained.

# 3 THE STRUCTURE OF THE DISSERTATION AND THE DESCRIPTION OF THE RESEARCH

The central question of my dissertation was to investigate where the public administration sector stands in terms of information security awareness, how would it be possible to effectively develop the willingness to apply information security rules and regulations, and how e-learning can be used in information security education. In order to improve the application of information security rules and the national level of cyber-awareness, it is not enough to provide purely information security related (technical) answers - complex problems require complex answers. In the first chapter, I explained the relevance and importance of the topic along these lines.

In the second chapter, I found that the interdisciplinary approach is not yet widespread in the Hungarian literature, so I could not find any reference to different motivational theories or assessments carried out by foreign researchers in this field. However, these new areas and theories have been on the horizon of researchers for more than a decade.

After reviewing the literature, I used a questionnaire to test my hypothesis. This survey required exploring and setting up novel methods. In the third chapter, I presented the subjects and methods of my research, in the framework of which I developed my own model based on the 5W+1H model, i.e. Kipling's Method. This model emphasizes that I identified the potential for improvement in a way that addresses both the regulatory and human factors in order to achieve a higher level of information security awareness, which is not only in our personal interest but also in the interest of the PUBLIC.

The model can be a support tool for an information security awareness development program, and can help individuals to learn how to effectively master written policies through training. I have used this model in face-to-face training sessions, testing its effectiveness on a sample of thousands of people. I have also used this model to design and create e-learning materials. I have analyzed the case studies and results of three such e-learning courses on a sample of several thousand participants, and the results have demonstrated its validity.

In the fourth chapter, I analyzed the responses to the self-report questionnaires using several statistical methods. Using the results of the questionnaire, I identified the gap between the public administration sector and the business sector in terms of information security awareness, which I also verified using statistical methods. As a result of the research, I supplemented the questionnaire studies with interview studies, as well as conducted live classroom training sessions, created e-learning course materials and tested them all. My hypothesis was that better rule understanding, better acceptance, implies greater willingness to follow and apply rules. The results of my research supported this, the reason for this might be that one's congruent behavior is easier to change in a live situation, while experiencing it first-hand for oneself.

The study also showed that live, attendance-based teaching is the most effective. Interactive feedback can play an important role in this. In the case of an active group, by asking questions that have been withheld (unasked, unanswered) for a longer period of time, group members actually support each other. While not as much change was detected in the case of e-learning training, it is possible to examine and detect medium-term changes, given other factors and an appropriate choice of indicators, if assessments and feedback are available from a wide range of public administration, in addition to central coordination. Building on the professional vocabulary introduced is one way of making the subsequent phases of rule application practice more inclusive once a common language and baseline has been established.

The conclusions and recommendations of this dissertation, which are presented in chapter five, may also help to address, at least in part, the fundamental dilemma of information security leadership training itself, namely how to increase the leadership effectiveness of information security leaders in the public administration sector. Leadership effectiveness can be increased if assessment results are available; it is possible to obtain results on the target area proportional to the risks taken. As an information security manager, scientific results may be used that show how to improve compliance (with regulations). The main novelty of this dissertation is its approach, a gap-filling analysis of literature on more than just information security, which extends the boundaries of the field. I have fully circumscribed the research problem posed at the outset, I set up my own model to examine the subject area and finally answered the questions raised.

In my dissertation, I highlight the roots that, if understood and explored, can be the basis for the transformation needed to change the insidious, bad practices and group norms that lie deep within. One of these is the way in which information security policies are issued, and the lack of support in their realization.

# 4 SUMMARISED CONCLUSIONS

Based on my first hypothesis, and rejecting it, there is a gap in information security awareness in the public administration sector compared to the business sector.

To measure awareness, I chose a questionnaire to survey password usage habits. The password (in general) as an authentication tool and is an excellent indicator of the level of information security awareness, and of the practice of applying the rules, because it is quantifiable, measurable and comparable. Many of the issues of confidentiality, integrity, availability with respect to information security, but at least confidentiality, are typically achieved by some form of access control, some authentication device such as a password. The use of authentication tools is widespread, perhaps it could be argued that there is no place where they are not used - perhaps the only case being public information. Therefore, the password is suitable both for large-scale assessment and, through its quantification, for generating time-series of measurement points, and also tracking changes in the application practices of information security rules through its variation (or lack thereof).

I found that the level of information security awareness in the Hungarian public administration sector is lagging behind compared to the Hungarian business sector, i.e. I rejected H1.

In order to increase information security awareness and compliance, there are a number of different options for work organizations, which are not limited to live training and e-learning. I have developed a model that is generally applicable to the many possible solutions for any communication channel. I applied this model during the assessments I carried out in two different work organizations for live training and e-learning.

My second hypothesis is that the practice of information security rule application can be more effectively developed through attendance-based live training compared to written rules, for which I used the number of reporting incidents as an indicator.

I found that the practice of information security rule application can be more effectively developed in the context of attendance-based training compared to written regulation, i.e. I considered my second hypothesis (H2) to be proven acceptable.

Then, based on my third hypothesis, I investigated whether the practice of information security rule application can be developed in the context of e-learning education. Can a significant change be demonstrated using my chosen indicator?

I examined the relationship between the intervals before and after the publication of the information security policies and regulations as well as the intervals before and after the publication of e-learning materials and the number of user notifications. Statistical tests showed no significant difference (F=1.126, p=0.303) in the number of notifications between policy publication and e-learning training. For the section without regulations, the difference cannot be tested as there is insufficient data. However, when looking at other possible indicators, a significant change in volume was found.

Although no correlation could be detected by statistical tests, I would like to stress why this observation is of paramount importance. Looking at the quantifiable values in a given work organization: compared to an average of 400 openings per month for the entire repository, here we measured thousands of cases of voluntary learning and task solving and thousands of feedbacks in addition to thousands of views. In addition, in the case of the e-learning module, which was completed voluntarily and on the basis of internal motivation, around 3,000 people completed the course material, then voluntarily took an exam, sometimes corrected it several times, completed it again and completed the questionnaire, which also provides feedback on voluntary basis. The optional e-learning training and related activities developed on the basis of my model reached (voluntarily) about 60% of the employees in the organization surveyed. I found that the practice of information security policy application can be developed through e-learning training, however, when comparing the results with the results of written policy application, the difference is not statistically significant, i.e. my third hypothesis (H3) is rejected. At the same time, I consider it of great importance that the 3 different information security training curricula designed and implemented on the basis of my model (not communicated as compulsory, but as interesting and applicable in a private context), were voluntarily processed by the participants in large numbers. Further assessment and studies would be worthwhile to investigate the significance (if any) of the way in which building on the technical vocabulary carefully introduced here speeds up, supports and makes participants more receptive towards further phases of the rule application practice. It is also possible to examine whether other indicators should be chosen or other surveys should be conducted through other questionnaires in the future.

## 5 NEW SCIENTIFIC FINDINGS

In my thesis first I assessed the level of information security in the Hungarian public administration sector. I developed my own questionnaire based on the information security models found during the literature review and based on my several years of experience in university and other (SIP) education. This questionnaire consisted of three parts: a demographic block, a password management block and an ICT skills block. I also used this questionnaire to demonstrate that password management habits (the use of passwords as a means of authentication) can be good indicators for measuring information security awareness. It can be used to identify, in part, information security risks, knowledge levels and willingness to comply (i.e. follow rules). The questionnaire was designed to identify relevant and salient risks related to identification and password management. The risks identified may be suitable for future use by information security professionals or for uniform consideration across a broad spectrum of public administration.

Using the information security questionnaire that I developed, I surveyed the level of information security in the Hungarian public administration sector. I evaluated the survey and found that the public administration sector is lagging behind the business sector in terms of information security (considering password usage as an indicator of information security).

A total of 1,243 people completed the questionnaire both from the business and public administration sectors (together). Using a Likert scale, quantifiable scores and free-text fields, the questionnaire collected quantifiable data on demographics, information security and ICT skills. Some variables were used to form a composite index. After quantification of some scale-type questions, the applied index and free-text fields, the scientific evaluation of all these data revealed that there is a lag in information security awareness in the Hungarian public administration. To support my thesis, I also used the raw data from the 2013 Illéssy, Nemeslaki, Som research, re-evaluated these unevaluated and unpublished data, which did not support my thesis and provided information for a better understanding of the results.

In my research, I applied a novel model to public administration that I developed.

In my research I reviewed the relevant international and national literature. I have identified a number of models and environmental drivers and reviewed the international literature in relation to my research. In addition to the models, I have also addressed causes and organizational factors that have not yet been investigated in the Hungarian literature. In doing so, I found that many models and scientific studies and approaches are not even mentioned in the Hungarian literature. These novel approaches and models coincided with my research and my established observations of educational methodology. I applied this novel approach together with the theories and models from the literature that I have identified to public administration in my research. I would like to emphasize that the significant and positive change here is the development of the educational model and methodology as well as their application, the assessment results of which I have presented in my dissertation.

Through my research, a research questionnaire through which data was collected during my years of teaching at the NKE EIV, my educational experience in the Safer Internet Program and in the business sector, I developed a model for the implementation of information security awareness behavior and a sample presentation based on my model. Three e-learning materials have been developed based on my model. These e-learning materials have been applied, tested, assessed and scientifically evaluated. In addition, I processed international literature partially in Hungarian but also on interdisciplinary fields (in part). Among the factors of human components influencing behavior, I considered the following: the Theory of Planned Behavior (TPB), the General Deterrence Theory (GDT), the Protection Motivation Theory (PMT), and the Technology Acceptance Model (TAM). However, in addition to these, there are more than 54 similar theories that explain the human propensity to follow rules, to apply rules, and decisions-making mechanisms in some way. Other interdisciplinary factors such as knowledge management, personal awareness preferences, or deterrence and restraint models can also be included. As a hard factor, I have examined regulation in my dissertation with an international literature review. With regard to information security regulation (within work organizations), I have formulated a number of recommendations that can effectively support the willingness to (understand and) comply with information security rules within an organization. I have quantified and presented my observations on the knowledge and awareness of information security policies in the presented research, where possible. I have formulated suggestions as to which aspects should be applied, changed and developed in relation to the design, implementation, communication and content of the policies, - that (based on my observations) are currently and typically not applied.

I have actually drawn on the international literature in both areas to develop my model. However, in many cases the literature presented anonymous organizations and case studies, and it was not possible to determine whether they were operating in the public administration sector or if they were other types of work organizations. In general, however, they all involved white-collar workers working in computerized work environments, which includes public administration as well. In the case of one company, although it has manufacturing capacity, i.e. it has employees who do not or typically do not work on computers, these jobs were not included in the research, as I only included employees working with computers. Thus, because of the similar jobs (computerized white-collar jobs), my research results are definitely relevant for public administration as well.

This model has the potential to have a significant impact on the willingness to comply with the rules, and thus to put the information security principles set out in the policy to practice.

I have applied the model I developed and presented in my dissertation to both live and e-learning trainings. I measured its applicability and the results of its application on a sample of several thousand participants. Its innovative and interdisciplinary approach, (which is not exclusively information security oriented), can support the implementation of awareness strategies, programs, education and training more effectively. It provides management and the information security profession with tools that can be applied to achieve significant and positive change. The model does not focus exclusively on the technical message, but also puts equal emphasis on the factors surrounding it. The model does not simply answer the questions 'Why?' and 'What?' but also focuses on giving a clear answer to 'How?', 'To whom?', 'When?', 'Where?' and 'Who?' and in the same time places emphasis on assessment and treats all of the foregoing equally important to the outcome. The model implies, (one might even say it guarantees), the success of the program because of the assessment, feedback and cyclicality factors, which also implies the potential for improvement in information security training.

I tested my sample presentation based on this model on a sample of around 4,500 people. The results show that attendance-based training is effective and achieves measurable results in the practice of compliance with rules. The number of notifications has increased, which means that participants are consciously applying their new knowledge. Effective results can be achieved in a relatively short time; whereas no such excessive values have been demonstrated for e-learning. It is conceivable that e-learning, through some form of it, could be effective in the longer term, although it does not promise similar impact in terms of numbers.

I have shown that education can improve information security awareness and compliance (with regulations).

I have demonstrated that by applying my model, information security education can lead to positive changes in awareness and compliance behavior in addition to knowledge regarding information security regulations. I tested this model presentation on a sample of about 4,500 people by means of assessment through a questionnaire before and after the actual training course held for a smaller group. On this sample, there was a quantifiable demonstrable effect on users' information security awareness behavior, as those who attended the training had a significant increase in information security awareness and willingness to follow the rules; and they applied the rules in their daily practice. I also applied my model to the development of e-learning materials; no significant positive change was statistically detectable on the resulting data, but there was a significant breakthrough in terms of course evaluation, feedback and number of staff mobilized.

Compliance Check Distance, (CCD), the development of a way to manage the risk from non-compliance practices, was a collateral result of the research. This initial empirical observation was later consciously applied and investigated. The use of CCD (provided through "live" training) as an informal channel can greatly assist in the identification of existing risks in the regulatory environment.

Non-compliances can be dealt with in an ex ante, exploratory (preventive) or ex post (detective and corrective actions) manner. According to standard, a certification requires to identify an area for improvement each year. However, these do not address the questions of when is something being assessed for an exact reason and what that reason is. Also, if the assessment results are good, if everything is found to be functioning well, why should it be re-tested, why should it be changed? If you have there is a practice and a method of assessment that works, why change it? But would it not be necessary to check whether we are assessing the right thing? After all, “we must realize, however, that the fact that an assessment instrument is frequently used is not in itself a guarantee of reliability” (Babbie 2001). It is possible that we are assessing the wrong thing from the wrong perspective, and it is possible that the whole process contains errors despite the audit. Timely detection of all these insidiously increasing risks can be helped by the assessment method borrowed from the business sector that is already in use in business processes. In areas with which there is no active communication, no regular feedback, we may develop even more processes that we do not understand, cannot assess correctly and thus cannot identify information security breaches or gaps. The model described in Chapter 3 (its application to attendance-based training), which includes feedback for these very reasons, can also be used to overcome these non-compliances. Maintaining compliance in this way can, however, be extremely costly if it is to be imposed on all work processes and recorded in the language of formal logic in a given system in a work organization. The model I have developed is not able to cover the entire Governance Risk management and Compliance (GRC) domain and to formally describe all risks, but it can be used to detect significant deviations in a timely manner, such that the output information obtained through the model can be used as input information to the CCD within the GRC domain, which can then be explored and managed.

## 6 PRACTICAL APPLICATION OF RESEARCH RESULTS

Education requiring “live” attendance allows for greater involvement and better understanding than making purely written regulations available. The e-learning curriculum is suitable for attracting attention and involving stakeholders, but did not significantly affect the willingness to follow rules. During “live” education, and following the lectures, the participants typically used the informal question and answer and clarification opportunity in the examined work organizations, while the questioning, which is also available but has to be initiated independently (individually, alone), was not used during e-learning. In the case of e-learning, on the other hand, it is possible to reach a large number of the target audience quickly and in a short time at low cost and to be able to create the foundations for later development quickly and for large masses. I also confirmed these findings with statistical tests. Significant changes can be achieved if education results in a greater willingness to follow the rules through stronger involvement and better understanding. It is possible to monitor and measure the change of this continuously with appropriate indicators. The developed model can be applied to both e-learning and live education. By supporting information security leaders working in public administration with a unified method of teaching and assessing, this can make a big difference.

**Results that can be utilized by the administrative sector**

It can support information security professionals working in public administration greatly if they can use a ready-made model, but even more so if there are centrally created learning materials available based on such model that can be easily shared within the work organization. It also helps if the tools for pre- and post-training assessments are similarly available, making them transparent at the administrative level, focusing on areas for improvement. Central coordination can increase efficiency because assessments and results can be compared in a larger volume and can also be analyzed better than if they were isolated or if only different, non-comparable data were available. Through better understanding and a greater willingness to follow the rules, all this will be used as an example to be followed in private life as well, so by opening “channels” to family members, relatives and acquaintances, the changes can cross strictly administrative boundaries and have a national impact.

**Results on the development of information security policies**

My research revealed that the knowledge and integration of the written regulations in the examined organizations is not supported. The preparation of role-based extracts, as highlighted in the literature and international research, is not widespread enough. As a practical result, with regard to the appropriate regulatory environment, the involvement of stakeholders in the regulatory process and the preparation of role-based extracts should be mentioned among the outstanding uses. The process of creating a regulatory environment, the usability of the end result and the subsequent impact on the willingness to follow rules also need to be given priority.

**Opportunity for change at national level**

There is no training in information security in the education program for those working in public education. As a further practical use, my information security results could be included in primary, secondary and tertiary education, and especially in university courses where postgraduate workers deal with minors. In addition to the basic qualifications of the information security officers working in the public administration, I highlighted the possibility of applying an international qualification and assessment system, which would also facilitate the comparability of training places and other training courses in Hungary. Furthermore, by applying my model, the efficiency of education and the willingness to follow rules can both be increased.

## 7 LIST OF MAJOR PUBLICATIONS

**Scientific Articles Published in Hungarian in Hungarian Journals:**

1. Som, Z. (2018) CCTV-rendszerek interoperabilitás és információbiztonsági megközelítésben, [CCTV Systems in an Interoperability and Information Security Approach], In: MAGYAR RENDÉSZET 17: 2 pp. 159-171.

2. Som, Z.; Papp, Gergely Z. (2016) Tudásfejlesztés a kiberbűnüldözésben – lehetőségek és kihívások, [Developing Knowledge in Cyber Law Enforcement – Opportunities and Challenges], In: Hadmérnök 11: 2 pp. 170-182., 13 p.

3. Illéssy, M.; Nemeslaki, A.; Som, Z. (2014) Elektronikus információbiztonság - tudatosság a magyar közigazgatásban, [Electronic Information Security Awareness in the Hungarian Public Administration], In: Információs Társadalom: Társadalomtudományi Folyóirat 14: 1 pp. 52-73., 22 p.

4. Som, Z. (2013) Kibertudatosság mint várható eredmény, a 2013. L. törvény távlati hatásai [Cyber Awareness as an Expected Result, The Long-term Effects of Act L of 2013]: structured and edited version of the paper presented at the conference in Budapest titled A Haza Szolgálatában ["In the Service of the Country"] on 25 October 2013, In: Társadalom és Honvédelem 17: 3-4 pp. 295-302.

5. Som, Z. (2013) A közigazgatási informatikai felelősök oktatásának kérdései, [Issues of Educating Administrative IT Managers], In: Hadmérnök 8: 4 pp. 223-237., 15 p.

**Books in Hungarian, as an author:**

1. Som, Z. (2014) Kockázatmenedzsment gyakorlat, [Risk Management Practice], Budapest, Magyarország: Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet (2014), 93 p.

2. Som, Z. (2014) Biztonság támogatása, [Supporting Security], Budapest, Magyarország: Nemzeti Közszolgálati Egyetem Vezető- és Továbbképzési Intézet, 66 p.

**Excerpts in Foreign Languages:**

1. Som, Z. (2014) Laws aiding cyber-security in the EU, In: Alexander, Balthasar; Hendrik, Hansen; Balázs, Kőnig; Robert, Müller-Török; Johannes, Pichler (ed.) Central and Eastern European eGov Days 2014: eGovernment: Driver or Stumbling Block for European Integration, Wien, Ausztria: Austrian Computer Society, (2014) pp. 115-126.

## 8 PROFESSIONAL CURRICULUM VITAE

Zoltán Som was born on July 19 in 1978 in Kazincbarcika. Hecurrently lives in Dunaharaszti with his family, wife and four children. He graduated from the Madách Imre Vocational High School in Gödöllő in 1998. He then graduated from the University of Szeged with a degree in mathematics, physics, computer science and programming mathematics. Following his advanced level English language exam, which he earned in June 2017, he also earned his basic level German language exam in July 2020.

He started working in the Rector's Office of the University of Szeged in 2003 as an IT specialist and then as an IT manager. The introduction of digital submissions of both the University Senate and other Rector's Cabinet materials are credited to his name. In order to learn about international good practice, he went to Finland under the Erasmus program and he also visited Greece with a scholarship. He was a lecturer of general informatics at the Juhász Gyula Faculty of Education of the University of Szeged for 6 semesters.

In 2010, he received the maximum score possible on his evaluation (required by the Act on the Legal Status of Public Servants) and a rating of "excellent" from the Rector of the University of Szeged. In addition to conducting scientific research, Zoltán has recently obtained several prestigious international information security certifications. He passed the ITIL exam. He then took the Certified Ethical Hacker Certification Exam at the EC Council. He has also earned two ISACA security certifications, one as a Certified Information Security Manager (CISM) and that one titled Certified in Risk and Information Systems Control (CRISC). In addition, he successfully completed the 'Cybersecurity and Its Ten Domains' course launched by Kennesaw State University on Coursera. He also passed the ISO 27001 Lead Auditor exam. Between 2013 and 2018, he was a member of the Szeged Chamber of Forensic Experts as an IT forensic expert.

In 2013, he applied to the Doctoral School of Public Administration at the National University of Public Administration, which was then launched for the first time in the country. Within the topic of security of electronic public administration systems, he also aimed to address in detail the human factors influencing information security.

Since 2013, he has been a doctoral student at the Doctoral School of Public Administration Sciences. He began his PhD studies in the field of information security. Later he was offered the opportunity to join the ÁROP-2.2.17 New Public Service Career Project and participate in the Review of the Electronic Information Security Vocational Training Course research project in which he took on an active role. He completed his doctoral comprehensive exam in July 2014, and in December 2016 he received his pre-degree certificate (stating that all course-units have been completed). In 2015, at the annual professional conference of the National Association of Doctoral Students entitled "Tavaszi Szél" ["Spring Wind"] held at the Eszterházy Károly Catholic University in Eger, he won the 1st place in the Public Administration Section with his paper titled „Az e-befogadás feltételrendszere és annak fejlesztése az információbiztonság tükrében" ["Conditions of E-admission and Its Development In the Light of Information Security"]. In addition to scientific and professional education, he also complies with a number of requests in the field of information security education and administration as a volunteer trainer.

In the 1st National Cyber Competition he supervised and professionally prepared a team of students from the National University of Public Administration, Faculty of Law Enforcement, who were awarded 4th place, for which he received a certificate of merit.

He has been participating in the European Union's Safer Internet Program as a volunteer trainer for several years.

He also complied with the requests of numerous administrative organizations. Thus, he held lectures on the topic of information security to the employees of the Szolnok Regional Court, the Csongrád-Csanád County Government Office, the Karcag District Court and the Szeged Regional Court.

He was a lecturer at the National University of Public Administration from the beginning of the specialized vocational training program for Electronic Information Security Managers in 2013 until 2020. He is the author of the following 2 textbooks – prepared within the framework of the knowledge-based public service advancement program: A biztonság támogatása [Supporting Security], and Kockázatmenedzsment gyakorlat [Risk Management Practice]. He has published the results of his research in several articles and presented them at both national and international conferences. Number of publications: 29, of which:
5 scientific articles published in Hungarian; 2 books published in Hungarian; 5 conference presentations in foreign language(s) and 7 conference presentations in Hungarian; 1 book excerpt in a foreign language and 3 book excerpts in Hungarian; 6 other publications.