NATIONAL UNIVERSITY OF PUBLIC SERVICE

Doctoral School of Public Administration Sciences

Krisztina Holló

Study on lack of security awareness, as a risk factor
with regard to the application of data protection and information security rules

Thesis Booklet of the Doctoral (PhD) Dissertation

Supervisors:

Dr Ferenc Leitold
College Teacher

Dr Attila Péterfalvi
Associate Professor

Budapest, 2022

TABLE OF CONTENT

1. SCIENTIFIC RESEARCH

1.1. DETERMINING THE SCIENTIFIC PROBLEM

Incidents of information systems can cause inconvenience in our lives and economic transactions, additional financial and trust losses, the serious damage to the European community and economic activities. The dissertation aims is to examine the impact of IT security awareness, the assessment of the IT risk factors focused on data protection and information security, and the lack of IT security awareness is managed in Hungary. Determining the title of the dissertation and the dogmatized localizing of the topic is served by emphasizing data protection and information security rules correlations. My background research focused on the field of public administration science but necessarily concerned the fields of the computer sciences and jurisprudence, which are significant for my results of research. The dissertation is submitted as a result of my research in the area of public administration science. Concerning the chosen complex research area and the attitude of interdisciplinary science, I defined additional clarification. Emphasising the relevant aspect of the dissertation, I focused on the examination of the lack of information security awareness. I also extended it to the correlation between data protection and information security principles and rules, their application and their acquainting. In addition, based on the development of information security awareness, I also focused on the drivers of incidents as a cause of shortages, their information security risk management and information security awareness correlates, and the effectiveness of relevant types of measures. In relation of tools and verifications, which are necessary to determine the dissertation results, I also focused on the economic aspects of data protection and information security incidents, the methods applied in IT risk analysis, the characteristics of information society such as human behaviour, and the ways to develop a digital culture in Europe. However, regarding the volume of the mentioned topics, I only applied them as the source and tools of my research verifications and part of my background research.

In conclusion, during my research, I sought an answer to the situation regarding Hungarian information security awareness, the specificities of shortfalls, their consequences and the possibilities of addressing them. In this context, in particular, the factors and results of the relevant processes are discussed in terms of data protection and information security, and information security awareness processes and relationship. Considering the mentioned processes and structure of the dissertation, its line started from the European and Hungarian data protection and information security regulation history, the situation of information security and awareness, and got to the need of develop legislation regarding data protection, information security and digital culture.

1.1.1. BACKGROUND AND RELEVANCE OF THE RESEARCH

With the appearance and development of communication technology, unique and unprecedented technological and cultural changes have taken place, and with the creation of the information theory in 1948, a new era was born fields of data protection. Information and knowledge has a significant key role in economy and social life, and nowadays, accelerated economy, society and technological processes are constantly shaping this. With rapid and secure information flow, the availability of supporting processes and technologies, the acquisition, dissemination and development of individual knowledge, both in the competitive and public sectors, have become essential. Our World is built on information systems to such an extent that it has been accompanied by a regulatory regime mainly information security standards and the General Data Protection Regulation (GDPR). Information, digital data and the technology built around them are inseparable. Computers, IT applications, systems and networks not only reflect the current state of technological development but also serve to protect our data. In this context, there is no hierarchy, *only a few* essential, fundamental factors with information and data at the centre, where data security and data protection are essential, which require the most advanced IT solutions at all quality levels. My research is based on the mentioned topic of data protection and information security problem fields.

1.1.2. THE TOPIC AND THE PURPOSE OF THE RESEARCH, AND THE RATIONALE

The significant role of IT is reflected in creation of e-government and its relation to public administration science. Information systems must ensure that electronic information is available, can be handled securely and is not compromised, which is the fundamental principle in the field of information security today. As my research topic, I chose a survey and analysis of data protection and the information security standards and regulations, the analysis of assessments to determine the information security level and the investigation of the potential development of information security awareness. Regarding the regulatory framework, I examined the General Data Protection Regulation (hereinafter GDPR), the Hungarian law of the right to informational self-determination and the freedom of information (hereinafter Infotv.), the Hungarian law of the electronic information security of state and local government institutes (hereinafter IBtv.), and the standard for information security management systems (hereinafter ISMS) and their requirements. All other standards and regulations were examined to support the background research and to validate the hypotheses. A detailed examination of regulations and standards are not part of the dissertation. Closely related to the topic is the examination of data protection and information security principles and rules applicable to the operation of the information system, and information security risk management, the analysis of the exploitability of the user behaviour. My research topic concerns the historical overview of information, the data protection and information security rules, the relevant legal instruments, and their evolution, provisions and recommendations related to data protection and information security regulation, the opportunities that information systems provide to the user community, the management of information assets, in particular the scope of personal data, user activities, actions that affect the functioning of information systems, malicious activities and the factors that cause them. During my research, I examined the fulfilment of data protection and information security principles and regulations, user awareness, and information security risk reports made by data of own cybersecurity company, other companies, and institutions.. In my research, I have not made a comprehensive analysis of the conceptual factors of cybersecurity and cyber defence, the type of data breaches and IT incidents. However, I presented cases and statistical data from the field of data protection and cyber defence as examples for the research topics to justify the legal basis for data protection and information security provisions. The focus of examinations is on personal data breaches, in particular data leakage, data theft, data loss, and incidents caused by *some* malicious code types as a results of which confidentiality obligation, data accessibility and integrity are compromised. Information security regulation (IBtv., ISO/IEC 27000) covers a great area. Due to the limitation on the scope of the dissertation, I will not specifically address the areas of internal organisation, physical and environmental security, security of supplier relationships, and business continuity planning (BCP). In this dissertation, I partly dealt with information security policies, human resource security, asset management, access control, (user responsibilities, system and application security), encryption measures, operational security, communication security, system development and maintenance (related topics are the development and maintenance of interoperability), information security incident management, and compliance (relevant legislation, intellectual property rights, protection of private and proprietary information, encryption measures) and information security investigations. In this dissertation, I published the results of the information security risk analysis conducted in research accompanied by some measures for the management of information security assets. Using my information security analyses and statistical data during five years in a small company, I have further investigated behaviour regarding security awareness using impact studies on IT systems and our environment. Thereby the dissertation includes official statistical data and references that are more than a few years old but essential for the research activity. In my research, I dealt only partially with the scope of IT-related attacks and threats that exploit user activity and IT-related technical solutions. However, these it is important to note that factors affect the data protection regulations and technical solutions, information security regulations and risk management, and the human factors. Regarding aspects of IT risk management, the methods for analysing and managing relevant threats, attack attempts and incidents are included in the dissertation, but study on these methods is not part of the document. In the dissertation, I do not deal with such IT solutions in the dissertation, for example, the achievements of the industrial revolution definition and solutions of artificial intelligence, and with the detailed definition and presentation of IT attack methods. It is not the subject of the dissertation to enumerate and examine the full range of categories, principles, rules and events relating to data protection, information and information security. For the purposes of this research, the focus was on specific user groups mainly the general user, data controller, data processor, system administrator, and the students. These groups were defined and examined through the incident approach, who direct and indirect caused the incident and who can become a potential victim. The definition of age and sex is irrelevant for the purpose of this analysis. The Information Security Awareness Program formulated in the context of Awareness Practice as a university (NKE) note identifies the importance of user levels. However, the mandatory distance learning methods introduced as a result of COVID-19 and the experience gained from them have completely redefined digital literacy needs. Children and non-IT-educated average users without higher education qualifications generally lack the IT and information security knowledge to provide an adequate level of digital literacy to support distance learning. Learning from the pandemic, children must also be prepared for the dangers of the virtual world, not only for the benefits of its use. Based on the experiences, the deficiencies of the system has to be corrected, not only because children in the first grade already use smartphones, but because they are considered general users of the organisation, such as a primary school. Another significant user group includes pensioners, who receive user access to the Hungarian central identification (Government Gateway) and banking systems. Those user levels were examined in the dissertation and were part of the statistical sampling for my research based on the given event, data analysis and document examination so that analysis of the population of pensioners is not part of my investigation. However, it is part of the general user level (hereinafter referred to as the "ÁFSZK model") that I have identified. In addition, citizens' IT security awareness is influenced by the state, development, and reliability of the information system, as well as by the activity of hacker actors in cyberspace, the damage they cause and the extent of breaches. Various online studies, guidance, and data protection statement on how to prevent attacks are designed to help the user community to strengthen security-conscious behaviour. A major objective for the development of public service systems is to create a set criteria that ensures the balanced, efficient and safe cooperation of the different public service levels (interoperability). The Zoltán Magyary Programme for the Development of Public Administration can be linked to the topic of information security in public services, as some of its chapters have also included information security aspects. Compliance with data protection and information security regulations can be monitored through internal and external control processes so that results of system audit and the feedback from the educational activities results can show weaknesses areas to be addressed or improved. I have been investigating well-structured psychological deception and attack methods and techniques since 2008, which take advantage of the security awareness lack of the human factor. The dissertation is an attempt to verify the hypothesis, to present the current state of information security, data protection in public administration and protection of private data, to make an analysis from the perspective of information security awareness, and to explore the links between data protection, information security and information security awareness. This is intended to identify the lack of information security awareness, information security risk factors and development possibilities, so that I can support digital literacy improvements in Hungary.

1.2. STRUCTURE OF THE DISSERTATION

The main topic of the dissertation is the investigation of information security awareness, and related development possibilities, closely linked to a review of the history of information, data protection law, analysis of information security events and statistics, the information security risk management, and an overview of the *„human factor”* and factors influencing the development of digital literacy. The dissertation considers, formal characteristics of preindustrial, industrial and post-industrial societies from an information history and data protection law perspective. The main focus is on the development of legal institutions related to information security and data protection from copyright to data protection and information security, as well as the Rome Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR), the current and relevant domestic and European Union legislation on data protection and information security (1950-2021), moreover statistical data on data protection and information security incidents surveys (ENISA), relevant decisions by public authorities (as Hungarian National Authority for Data Protection and Freedom of Information, hereinafter NAIH), domestic statistics (as National Cyber Defense Institute of the National Security Service, hereinafter NBSz NKI), and conclusions of incidents (for the period 2000-2021) , statistical data and conclusions of information security risk assessment and risk management (for the period 2015-2021), examination and research data on the "*human factor*" of accidents (for the period 1990-2020), and requirements for the development of digital literacy (for the period 2017-2021). Concerning the dissertation, I finished the examination and summary of source documents at the end of February 2022 and the modifications based on the first review were finalised at the beginning of August 2022. The findings on scientific results are based on the statistical data and documents available to me at the end of March 2022. I have structured the chapters, verified the hypotheses and established the theses according to the main considerations above.

1.3. HYPOTHESES OF THE DISSERTATION

During my research, I formulated the following hypotheses:

- According to my first hypothesis (H1), I assume that the development of data protection and information security principles and legal provisions in Hungary is consistent with the recommendations of international standard-setting institutions and European regulations.
- According to my second hypothesis (H2), I assume that the lack of user's information security awareness facilitates the occurrence of data protection breaches, thus and cybercriminal activities.
- According to my third hypothesis (H3), I assume that the awareness of data protection and information security principles and regulations in Hungary is effective in influencing the development of user information security awareness.
- According to my fourth hypothesis (H4), I assume that the information security awareness system should be made available not only in the digital skills training programs to all age groups and should be introduced and implemented in all disciplines.

With the findings of the thesis, I would like to reinforce the hypothesis that increasing user information security awareness based on the principles of data protection and information security contributes greatly to the reinforcement of our information system, most important, our domestic public administration system. On the other hand, its lack or weakness increase weak points in our information systems, which can make them more vulnerable and exploitable.

1.4. RESEARCH METHODOLOGY

During my research, I used a variety of methods, in a particular document and content examination processing information history and legal history analysing data protection and information security legal factors, general and comparative chronological analysis; examining international and domestic data protection guidelines, principles and laws and international information security recommendations in each chapter. I used qualitative and quantitative methods (in the case of ISMS analysis quality management methods in chapter four), comparative analysis (examining international and domestic legislation in chapter two) statistical data and database analysis (for risk management, in chapters four and five), and empirical research (using reasonableness, mathematical logic, and observation to strive objectivity and accuracy, in each chapter), and research-relevant definitions (in the area of information security). Given that my research requires a consistent use of terminology, I considered it necessary to present and define the correlations.

Given the fact that my research focused on the lack of information security awareness, its triggers and consequences, a simple finding based on a questionnaire survey of the population was no longer sufficient to establish the results on the state of digital literacy and to summarise the needs for improvement. For this reason, I considered it necessary to carry out my own statistical analysis based primarily on the authentic data collected by the authorities (ENISA, NAIH, NBSz NKI).

2. DESCRIPTION OF THE RESEARCH BY CHAPTER

The dissertation consists of six chapters. The chapter one is the introduction which includes the description of the background research, the topicality and the purposes, the justification for the choice of the topic, the formulation of the scientific problem, the structure of the dissertation, the hypothesis of the study and the methods used to prove them. The chapter six includes the summary findings, conclusions, the verification of the hypotheses, the summary of new scientific results and the recommendations for further development and utilizations. A concise description of the research and presentation of the studies in the thesis, from chapter two to chapter five, is given below.

2.1. The importance of information, the legal history and regulatory regime of data protection and information security law history and their regulation system (second chapter two)

The chapter two includes the results of the analysis of the legal history and legislation on data protection, and information security necessary to prove my first hypothesis (H1). The hypothesis was proved by taking into account the methods of comparative analysis. In this chapter, I presented the most important data protection and information security legal institutions related to the concept of information. To use the technical terms related to the subtopic of information security awareness more accurately, I used the definitions and contexts which I have defined in the dissertation. During my research for this chapter, I examined the historical background and development, significance and context of international, primarily European Union, and, as examples, German and Hungarian data protection (GDPR, Federal Data Protection Act – Bundesdatenschutzgesetz – BDSG, Infotv.) and information security regulations (IBtv.), and standard recommendations (ISO/IEC 27001), legal instruments, and the necessity of the application of data protection principles and rules.

2.2. Significance of data protection, correlations between regulation and practice (chapter three)

In this chapter, among the applicable methods, I give priority to the use of prevention-type methods supported by data protection and information security regulations, and their usefulness as verified by my results of my research and the data protection statistics evaluated in this chapter. During my research, I primarily illustrate the need for compliance with data protection principles and information security rules through a statistical statement I have compiled based on a review of cases published by NAIH in publicly available data protection decisions. The statistical data from the international and domestic data protection cases examined highlight the importance of data protection rules and privacy impact assessment.

2.3. The rules of the information security management system (chapter four)

In the fourth chapter, I analysed the significance of the international and domestic information security rules both at international and domestic level. Using the statistical data on international and domestic information security incidents, I have demonstrated the necessity of applying information security standards and regulations at institutional level, and the harmful effects of ignoring the rules, and thus the cybercrime component of the proof of my second hypothesis (H2). Considering that the formulation of standards and the implementation of measures to strengthen information security concern not only private enterprises, and public institutions, but are in the interest of our nation as a whole, the starting point cannot be other than public administration and public authorities. In the course of the study, I illustrated the need for compliance with information security rules through the statistics on information security incidents the demonstration and applicability of an ISMS and information security risk management (ISRM). In my research, I took into consideration the taking effect of the GDPR and Hungarian regulations (Infotv.), and I examined separately the periods before and after . In relation to this period I looked at the impact and outcomes of the COVID-19 pandemic, the increased teleworking such as "home office" and information security events. For my research, I analysed the public and authenticated statistical data created by international and domestic scientific publications, authorities (in the dissertation: figure 14 - Statistical data most common incident types based on NKI data) and IT security enterprises, in order to verify the information security factors of my second (H2) and third (H3) hypotheses in particular, which I compared and analysed with information security data of the organisation I audited. I have used the document and content analysis, qualitative , quality management, in particular information security (ISMS) and risk analysis methods, comparative studies, statistical data analysis, and empirical research using mathematical logic to report the research findings in this chapter and to provide background research.

2.4. The role, status and effect of information security awareness (chapter five)

In surveys referred to in chapter five, I selected the events of personal data breaches through which I presented the verifications of the mathematical statistic , the level of information security awareness and the areas for improvement. For the analysis of personal data breaches it was necessary to conduct empirical method-based background research on the so-called "human factor" based on the empirical methods in the background research which is need for research of the risk analysis and information security awareness, additionally for the verification of the hypotheses three (H3) and four (H4). Using the mathematical research results, our research team had proved that during risk analysis, the user behaviour also has to be taken into consideration not only the protected IT system and the malicious activity (in the dissertation: figure 15 - influencing factors of the IT infrastructure). During my domestic research, I analysed the IT and information security activities of an enterprise where they developed not only software-supported information security research but also operated various IT systems. In my research, I applied the *common criteria* and the *requirements* of the ISO/IEC 27001 *standards for the introduction and operation* of the ISMS, the risk management (ISRM, RA such as inventory, vulnerability and potential threats), implementing actions (based on the *probability of occurrence* and *impact analysis*), as well as raising employee awareness and conducting the internal audit. The research has verified that by implementing meaningful measures, conducting annual ISRM and *internal audit*, the number of high risk, such as *vulnerability* and *potential threats* and *probability of occurrence* can be decreased (in the dissertation: figure 20 - Threat analysis and potential effects based on own risk analysis and impact assessment, 2020). Based on my research and risk management procedures conducted between 2015 and 2020, I found that the number of incidents can be decreased by 5-20 per cent by addressing vulnerabilities, preventing human errors from occurring and applying prevention methods (mainly information security methods, 54%) (in the dissertation: figure 21 - Types of measures required in the risk management action plan and figure 22 Risk management, distribution of acceptable risk, residual risk based on own research). During my research, I applied various methods to raise awareness of information security, in particular information security education, training, one-to-one consultation and interactive communication. My research results on security awareness have also been strengthened by the cases studied on the topic of risk management and the investigation of the incident in a travel agency published by NAIH.

3. SUMMARY FINDINGS AND CONCLUSIONS, NEW SCIENTIFIC RESULTS

Cyberspace-related difficulties such as vulnerabilities, security gaps and exploitable incidents now threaten not only the operation of organisations and public institutions but also the lives of households and thus our children, and cause serious economic and personal damage. Therefore, data protection and information security regulations cannot be ignored. Even prevention and protection, data protection and information security, measures against continuous attacks do not provide complete protection, but knowing the risks, and implementing actions designed accordingly can reduce the number of potential incidents.

3.1. Verification of hypotheses

Regarding verification of the hypothesis one (H1), the examination of the relevant legal history, historical overview, data protection and information security rules, and examination of the standards (chapter two) are indispensable. Considering the aspects of the research area, it is primarily necessary to position the topic, examine the relevant processes of data protection and information security regulation and their correlations in order to examine the state of information security awareness in relation to the legal requirements. The exploration and presentation of the historical, technical and legal relationship is essential since it is a unique symbiosis of legal institutions and technologies that has evolved from a very young discipline. As Hungary is a member of the European Union, we must comply with a number of EU laws, including the provisions of the General Data Protection Regulation. Therefore, the focus of the investigation had to be extended to international but most importantly the EU legal order with regard to the level of compliance of Hungary with the regulatory obligation and the extent to which our legislation is in line with international practice. In addition, it is necessary to take into account how other Member States, such as Germany, have implemented these tasks. During my research, I found that the Hungarian information security regulation (IBtv.) does not cover all legal entities, only states and government institutes. However, proving the hypothesis H1 and the conclusions I have drawn show that establishing and applying the relevant principles and provisions are crucial to ensure the protection of personal data. During the examination of the conceptual framework, I found that the scope of the concepts of the Ibtv is substantially broader, as it contains not only information protection and information security terms, but also statements on data protection. There is a redundancy, and some differences between the interpretative provisions of the two Hungarian regulations (such as Infotv and IBtv). With regard to Infotv, emphasising the Hungarian characteristics and the need for a code of conduct would be essential. There are much more varied definitions in terms of curricula and literature, and there is no consensus on the concept of information security awareness. It is essential to create and publish uniform Hungarian data protection and information security terminology, which need to be periodically reviewed and developed in line with IT development. Data protection, information security regulations and recommendations in standards facilitate their adaptation at institutional level, but unclear definitions result in misinterpretations of the legislation.. In the course of the research, I found that the application of the Hungarian data protection and information security regulations effectively influences the development of the information society. By applying the standards, the principles of confidentiality, integrity, availability and data protection for the information system are met. The consequence is the increase in confidentiality built on knowledge, information and IT, and the advancement of post-industrial society. The application of data protection and information security regulations in place and in force limits data collection, reduces the number of personal data breaches, and increases the information security level of the system. One of the legal basis of data protection and information security regulations is the personal data breach. The complex regulatory framework provides guidance for the design, maintenance, and protection of the IT system, and the lawful processing and transfer of data, moreover, for building public trust by penalising unlawful activities. Therefore, the development and application of data protection and information security regulations in a coherent way with IT processes is a factor that enhances citizen's confidence. The Hungarian regulations in line with EU legislative requirements provide protection for citizens' data, ensure data protection and information security rights, clearly define the tasks, rights and obligations of data controllers and processor, but need further development. A major factor in incidents, beyond the technological solutions, is the "human factor", which is a key component of the information system. The findings provide both indirect and inverse verification for the relationships between hypotheses H1 and H2 and H1 and H3. Hypothesis H2 suggests that the impact of a user information security awareness gap could potentially lead to data breach. The Primary focus of the study is the cause-and-effect relationship between hypotheses H1 and H2, the outcomes of the processes and deficits examined in hypotheses H1 and H2 such as the consequences of non-compliance. Moreover, studying the correlations between information security awareness, compliance and noncompliance including the relationship between information security awareness gaps and opportunities of cybercrime (H2). The results of the analysis of the data protection and information security statistics that I have verified that the human factor is an essential component and one of the factors influencing the level of information security in information systems. The development of this area shows an increasing level of information security, while its neglect shows a decreasing trend. The technical measures used in the processing must comply with data protection principles in particular in order to effectively achieve data minimisation and to comply with the requirements to incorporate safeguards necessary to protect the rights of data subjects. The investigation focused on the lack of information security awareness which can lead to more types of human error (such as *skill-based errors* and *mistakes*) and intentional harm, facilitates incidents, and supports cybercrime. I have also found that during cybercrime mainly exploits inadequate data control, particularly in terms of phishing and malicious software. These incidents caused significant damage in different sectors, such as healthcare, education, government, bank, industry and services. The cost of restoring the damage and reinforcing the level of protection is significant, and is therefore a factor damaging the economy. During the analysis, I demonstrated that combination of rule-based (ISO/IEC 27001, Infotv., IBtv.), IT and information security improvements, interoperability solutions, and developed technologies (such as AI) provide greater protection for our data and IT systems against increasing sophisticated attacks, and mitigate the effect of the incidents. A significant proportion of data breaches are cybercrime activities. The inverse and indirect finding related to hypothesis H2 is that improving information security awareness is one of the decreasing factors of cybercrime activity. I conclude that given the "*human error*" factors of the incidents, more complex privacy and information security awareness is essential to strengthen preventive information security processes. With the above-findings, I verified the causal relationship between hypotheses H2 and H3, and hypotheses H2 and H4.

Regarding the verification of hypothesis H3, the subject of the research is the comparison of the results, which are obtained from the examination of hypothesis H2 with information security risk management, and the effectiveness of awareness-focused measures and the analysing the correlation between the "human factor" and the information security risk management. The confirmation of the hypotheses H2 and H3 has resulted in overlaps in the analysis of the human factor effect. Hypothesis H3 is supported by my own risk management, research results, statistical data processed by ENISA and studies cited by the organizations as well as the results of the NAIH case study. I have therefore proven my statement that raising awareness of the importance of data protection and improving information security awareness can reduce the exploitation of *human credulity*, the number of *mistakes*, omissions and deliberate damage, thereby strengthening the level of information security in the organization. The need for awareness-raising is reinforced by the fact, that basic and advanced IT courses organized by higher education, institutions, focus on data protection, security technology, and information security principles and solutions, which can be put into practice. The direction is appropriate and needs to be sustained in the future however, the statistics from my research presented in the dissertation and studies show that the time and activities devoted to information security awareness are not enough.

Regarding hypothesis H4 and based on the results which are obtained during the verification of hypotheses H2 and H3, , the study will focus on the state of digital culture, the program for increasing information security awareness, its effectiveness, the identification of additional information security awareness levels based on the program, and examination of the age groups involved in the topics. I have also taken into account the European Union's digital literacy proposals to verify hypothesis H4. Focusing on the "human factor", I found, that digital competence in information security skills can be developed from childhood to old age, but it is a very time-consuming procedure. Information security training should be made available to students at all levels of education and for all age groups, thus contributing to consolidate the creation and development of digital literacy and "cyber hygiene". The information security awareness of citizens working for companies and in the public sector must be continuously developed, and face-to-face and online, corporate group or individual consultations, training and education have to be integrated into everyday work processes. During the information security audit, through analysis of the human factor of the information security awareness, incident investigations and statistics and the IT training, I experienced that despite the fact that an institute or company has IT security policies management instructions and procedures in place for users, the lack or insufficient of activity contributes to the decrease of the security awareness.

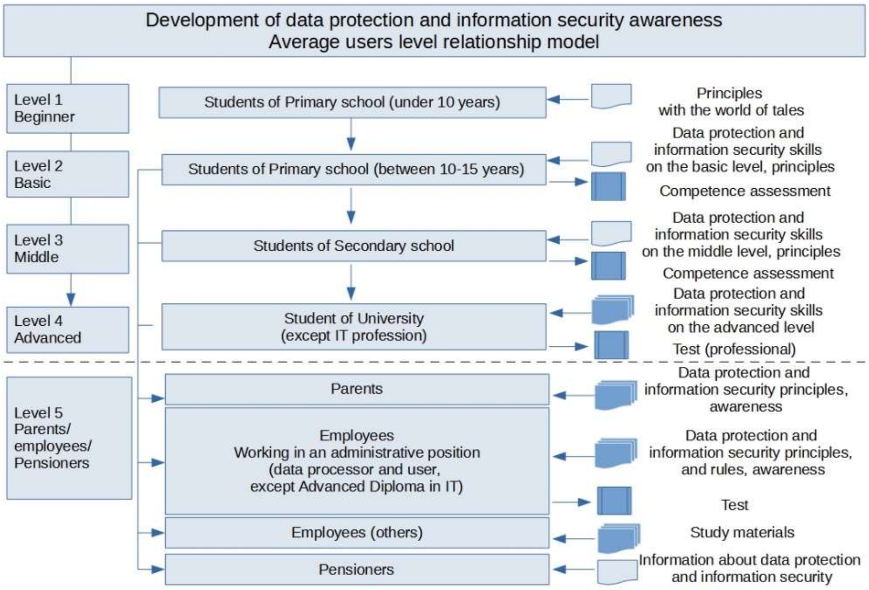
Development of data protection and information security awareness
Average users level relationship model
Level 1 Beginner
Level 2 Basic
Level 3 Middle
Level 4 Advanced
Level 5 Parents/ employees/ Pensioners
Students of Primary school (under 10 years)
Students of Primary school (between 10-15 years)
Students of Secondary school
Student of University (except IT profession)
Parents
Employees Working in an administrative position (data processor and user, except Advanced Diploma in IT)
Employees (others)
Pensioners
Principles with the world of tales
Data protection and information security skills on the basic level, principles
Competence assessment
Data protection and information security skills on the middle level, principles
Competence assessment
Data protection and information security skills on the advanced level
Test (professional)
Data protection and information security principles, awareness
Data protection and information security principles, and rules, awareness
Test
Study materials
Information about data protection and information security

Figure 1, Development of data protection and information security awareness, Average users level relationship model (ÁFSZK - AURship), own editing (figure 23 in the dissertation)

I have found that children, as well as the average non IT-educated user without tertiary qualifications (level 5+1: General User Level), should be provided with the appropriate level and number of hours of digital, privacy and information security training. Based on the proven hypotheses, I defined the model for the development of data protection and information security awareness (figure 23 in the dissertation on the basis of which I distinguished five levels. Everyone should have basic data protection competence, to ensure the effective development of user information security awareness skills.

3.2. New scientific results

Based on the dissertation and the verifications of the hypotheses I formulated the following theses:

T1a Hungarian legal provisions on data protection and information security are in line with international information security standards and the General Data Protection Regulation but the correlation of interpretative provisions is an area for improvement.

In the context of hypothesis H1, I have concluded that creating and applying the related principles and provisions is essential to ensure the protection of personal data. In addition, domestic data protection and information security regulations are in line with international provisions, the GDPR, the relevant provisions of the BDSG (Federal Data Protection Act – Bundesdatenschutzgesetz) and recommendations of the International Information Security Management System (ISMS). At the same time, the interpretative provisions of the laws are sometimes inconsistent, there is a lack of declaration of key terms and those that do exist need to be clarified. As regards consistency, the redundt definitions need to be improved. The general interpretative provisions of data protections should be included in the Infotv, and the general interpretative provisions of information- and cybersecurity should be included in the IBtv. In conclusion, according to the current scientific view, it is necessary to introduce uniform Hungarian general interpretative provisions on data protection and information security along with the definition of correlation of the relevant technical terms.

T1b The scope area of the Hungarian information security regulations has a significant deficiency.

Regarding the scope of the IBtv does not apply to all legal entities, it is necessary to extend the information security legal requirements to enterprises with 250 or more employees and self-employed persons.

T1c Support for citizens through data protection and information security rules and awareness-raising are confidence boosters for citizens, a human factor influencer and indirectly a risk reduction factor.

Thesis T1c is formulated on the basis of the correlations between H1 and H2, and between H1 and H3.

T2a Depending on the probability of occurrence of data protection events, the lack of user information security awareness in relation to the "human factor", in particular the "human error" rate can indirectly lead to data breaches.

T2b A significant part of data breaches originates from cybercrime activities.

T2c The development of information security awareness is a factor in reducing cybercriminal activity.

T2d Complex privacy and information security awareness training is essential for the effectiveness of preventive information security processes.

Theses T2 were established as a result of the verification of hypotheses H2, using the correlations between the conclusions of hypothesis H2 and H3, and as a result, and I created the ÁFSZK model as a result (figure 23 in the dissertation).

T3a Raising awareness of data protection and information security principles and regulations effectively influence the development of user information security awareness in Hungary.

T3b In the context of the relationship model of general user level related to the development of data protection and information security awareness, training and feedback processes are immature in Hungary.

Based on the verification of the hypotheses H3, I have established the theses T3, which states that awareness-raising processes built on the solid foundation of data protection and information security principles need to be strengthened and developed.

T4a System of data protection and information security awareness should be made available not only in IT education but to all age groups, moreover it should be introduced and implemented in all fields of expertise.

T4b Due to the lack of an appropriate level of data protection and information security education , the data subject can impossibly be had digital skills at the expected level, leading to a significant lack of information security awareness.

The formulation of the theses T4 is the result of a correlation test of the hypotheses H2, H3 and H4 justification.

T4c Data protection and information security principles should be made available to all ages, to ensure that users' information security awareness develops effectively, and that digital literacy develops at an appropriate pace in line with IT progress.

Based on the verification of the hypotheses H4, I determined that a system of information security awareness needs to be implemented and operated, which affects all age groups in education and various fields of expertise.

T4d Lack of feedback leads to questionable outcomes and decision making based on inaccurate facts-, which is a significant risk factor.

My research results and the presented ÁFSZK model support the significance of feedback, which I determined based on verifications of hypotheses H1-H4.

4. RECOMMENDATIONS FOR THE PRACTICAL UTILIZATION OF THE NEW RESEARCH RESULTS

The dissertation gives an opportunity to apply skills development for information security awareness for all ages. The findings suggest that in the context of digital culture (IT) education in primary and secondary schools the themes could be extended to include awareness-raising methods and curricula (data security, data protection and cybersecurity principles, and the Hungarian codes of conduct). It must be adjusted to actual demand, subject theme and methods. The results of information security (InfoSec) tests taken by the prospective students at the time of admission may be decisive in determining whether InfoSec training is required or not. Thereby, the training level can be provided based on the digital competence at local level.

4.1. Information security awareness suggestion for kids

Nowadays, there is an increasing focus on children's cybersecurity, examining children's vulnerability and risks to various online threats. The application of information security methods under the age of ten is a controversial topic even among professionals. However, children as young as four and seven years who already understand the lessons of tales can be introduced to the world of security, the world of ugly-beautiful and bad-good, whether it is the Internet, an application and a favourite tale. If we accept that children can instinctively make a difference between right and wrong can be taught through stories, their digital skills can also be developed through play and educational stories. In the thesis, I have proposed a solution to reinforce some skill areas with digital tools and support the acquisition of information security terminology (such as teaching CIA principles with keywords, symbols, and cartoons). An information security concept can be created for pre-school children, in particular identity protection, the ability to save, ask for and accept the help cyberattacks – even in transport, recognizing inauthentic content, developing curiosity about the digital world, creating a good stewardship attitude in the digital world, and cyber footprint awareness. The application of the recommendations in a pre-school setting is better supported by professionals and pre-school teachers. In this project, it is essential, that parents must be involved in their children's education, as they are the ones who give smartphones to their children to keep in touch.

4.2. Information security awareness suggestion for parents

Given the fact that parents monitor their children's studies, it is advisable to use group parent-teacher meetings as an opportunity to use information security awareness tools. Topics can include in particular an overview of data protection and CIA principles with school examples, case studies, and supporting learning with smart devices.

4.3. Suggestion for new research, and regulation development

The results obtained in the thesis are suitable for further development of research, such as creating a BSC strategy map related to information security, elaborating methods for the development of children's security-conscious thinking, extending the scope of the IBtv to companies with 250 or more employees, and creating the Hungarian codes of conduct for public administration.

PUBLICATION LIST OF THE DOCTORAL CANDIDATE

[1.] Eszter OROSZI , Krisztina GYŐRFFY: Information security for egovernment social media marketing and citizen interaction, Central and Eastern European eIDem and eIGov Days 2016: Multi-Level (e)Governance: Is ICT a means to enhance transparency and democracy?, Budapest, 2016.

[2.] Ferenc, LEITOLD, Kálmán HADARICS , Eszter OROSZI , Krisztina GYŐRFFY: Measuring the information security risk in an infrastructure, MALWARE 2015 10th International Conference on Malicious and Unwanted Software, Puerto Rico, 2015

[3.] Ferenc LEITOLD, Krisztina GYŐRFFYNÉ HOLLÓ, Zoltán KIRÁLY, Quantitative metrics characterizing malicious samples, In: Cyril, Onwubiko; Pierangelo, Rosati; Aunshul, Rege; Arnau, Erola; Xavier, Bellekens; Hanan, Hindy; Martin Gilje, Jaatun (szerk.) Cyber Science, CyberSA for Trustworthy and Transparent Artificial Intelligence (AI), Dublin, Írország: Center for Multidisciplinary Research, Innovation and Collaboration 2021. pp. 82-83., 2 p.

[4.] GYŐRFFYNÉ HOLLÓ Krisztina: Az információbiztonság jelentősége és története, GRADUS Vol 8, No 2 (2021), John von Neumann University, Hungary, Kecskemét

[5.] GYŐRFFYNÉ HOLLÓ Krisztina, Információbiztonság, avagy incidens kontra biztonságtudatos viselkedés, INFOKOMMUNIKÁCIÓ ÉS JOG 18., 76 pp. 17-23. 7 p., 2021.

[6.] GYŐRFFYNÉ HOLLÓ Krisztina, Az érintés nélküli adatgyűjtés kockázatai és a kockázatszámítás módszerei, DUNAKAVICS 9 : 8 pp. 77-97. , 21 p., 2021.

[7.] GYŐRFFYNÉ HOLLÓ Krisztina, Közszolgálati információs rendszerek interoperabilitási nehézségeinek megoldása, DUNAKAVICS 2021. IX. évfolyam II. szám pp. 21-40. , 19 p., 2021.

[8.] GYŐRFFYNÉ HOLLÓ Krisztina, LEITOLD Ferenc: Felhasználókkal kapcsolatos információbiztonsági intézkedések kezelése a GDPR tükrében, Hétpecsétes történetek 2,5 - a GDPR antológia, Budapest, 2018.

[9.] GYŐRFFYNÉ HOLLÓ Krisztina, Az információbiztonsági sebezhetőségek tényezőinek vizsgálata: A „humán faktor", In: Váraljai, Mariann (szerk.) INFORMATIKA KORSZERŰ TECHNIKÁI KONFERENCIA 2021 „Jövőformáló tudomány" „Fenntarthatóság és digitalizáció" Dunaújváros 2021. november 9.: DUE Press (2021) 80 p. p. 40

[10.] GYŐRFFYNÉ HOLLÓ Krisztina, Információbiztonság, avagy megéri kockáztatni? In: Nagy, Bálint; Katona, József AZ INFORMATIKA KORSZERŰ TECHNIKÁI KONFERENCIA 2020 : Jövőformáló tudomány programfüzet és absztraktkötet Dunaújváros, 2020. november 9-10., Dunaújváros, DUE Press 2020. 48 p.p. 22

[11.] GYŐRFFYNÉ HOLLÓ Krisztina, Az információbiztonsági tudatos viselkedés az incidensek elkerülésének egyik tényezője, DUNAKAVICS 8 : 12 pp. 5-18. , 14 p. 2020.

[12.] HADARICS, K., GYORFFY, K., Nagy, B., BOGNAR, L., ARROTT, A., LEITOLD, F., Mathematical Model of Distributed Vulnerability Assessement, Security and Protection of Information 2017, University of Defence, IDET BRNO, Czech Republic, 2017

[13.] Krisztina GYŐRFFY, Ferenc LEITOLD , Anthony ARROTT: Individual awareness of cyber-security vulnerability – Citizen and public servant, CEE eDem and eGov Days 2017: Digital Divide in the Danube Region: Is it still significant in explaining ICT adoption in eDemocracy and eGovernment?, Budapest

[14.] Krisztina GYŐRFFYNÉ HOLLÓ: The Human Factors of the IT Risk Management, DUNAKAVICS, Dunaújvárosi Egyetem online folyóirata 2021. IX. évfolyam VII. szám, 47-61pp

[15.] Krisztina GYŐRFFYNÉ HOLLÓ, Adam KARISZTL: Domino effect and other models in the it process, GRADUS Vol. 8, NO 3, John von Neumann University, Hungary, Kecskemét, 2021.

PROFESSIONAL AND SCIENTIFIC BIOGRAPHY OF THE DOCTORAL CANDIDATE

Krisztina Holló obtained a grade college diploma in the course of Information Technology Engineering (BSc, in 2001) and an excellent university degree in Information Technology Engineering from the Faculty of Information Technology at the University of Pannonia (in 2008). She got a professional qualification of Engineer in Information Technology with a complementary Degree in Legal Studies at the Faculty of Law and Political Sciences Pázmány Péter Catholic University (in 2014). She has applied her study at more universities and companies, such as an information system and SAP developer at Semmelweis University (between 2001 and 2008), as an IT security expert and quality management officer, but now as an assistant lecturer and mentor at the University of Pannonia (since 2008). She has researched as an information security expert and ISMS lead auditor in Veszprém. She has worked as an instructor and e-seminar leader in the Electronic Information Security Manager postgraduate specialist training course at the National University of Public Service and as a visiting lecturer in the course of Data Protection and Quality assurance and audit of IT systems at the University of Dunaújváros. She studied at the Doctoral School of Public Administration Sciences National University of Public Service (between 2016 and 2021). She obtained an absolutory in 2021.