BÁNKI KÖZLEMÉNYEK
2. ÉVFOLYAM 1. SZÁM

What makes an information security training project successful?

Zsolt Szabó
Doctoral School on Safety and Security Sciences, Óbuda University
Budapest, Hungary
szabo.zsoltmihaly@phd.uni-obuda.hu

***Abstract* — Nowadays project management is a very important part of corporate culture. Organizations recognize that a modern and economical organization cannot be run and maintained without project management. Competitiveness requires processes to be planned, executed, checked and supervised; a basis for the survival of organizations is project management. In large international corporations and organizations, project planning has been considered important for a long time and in Hungary its importance is starting to be recognized. The Hungarian government has worked out an Infocommunications State Secretariat project management methodology in public administration and makes countless recommendations for organizing and running public administration organizations. Nowadays in state organizations, project management methodologies and their application is standard practice. IT security is keeping the IT components of organizational activities in the proper condition to achieve the goals. Security is an essential element of corporate operation – in an organization it is just as important as business conditions. Security is a complex concept; the individual areas are closely related and connected and depend on each other. Information security protects information from many threats (fire, water, other natural disasters, computer hacking, sabotage, software and hardware errors due to improper handling, viruses etc.) in order to ensure business continuity, minimize damage to business, and maximise the possibility of business and return on investment. The paper shows the tasks of project management through an information security training project, using concrete examples. All the selected examples have project-based planning and introduction, and represent project management-based thinking, but taking into account local expectations and exceptions.**

***Keywords*: project management, IT security, e-learning, information security training**

1 INTRODUCTION

We should strive to create complex organisational IT security to achieve business continuity, in which the processes of the individual areas are closely interconnected—their operation has an effect on the operation of the organisation [1] [2]. An IT project—based on its results—selects, introduces or develops IT solutions or information systems to realise the strategic goals of the organisation [3]. Since projects are not repeated under the same conditions, there are no universal recipes, only effective techniques that speed up implementation. Matching these to the project is a top priority for project management.

2 ABOUT PROJECT MANAGEMENT IN GENERAL

2.1 Project

A project consists of a multitude of subtasks, which constitute a process. Every task is a project that has a clearly defined goal, time, cost and expected performance. Based on the standards issued by the International Organisation for Standardisation (ISO), a possible definition of project is: A project is an individual process which is a group of activities undertaken, coordinated and controlled in order to achieve a set goal, and which has a clear starting and finish date and conforms to specific requirements, such as quality, resource and cost limits. In my paper I consider project organisational tasks within a timeframe, which probably could not be performed efficiently with the use of the routine basic functions of the organisation, due to their size, complexity, novelty or importance. The above characteristics require leaders to handle such tasks with a temporary organisational solution, specially focused on the successful execution of the project [4]. Fig. 1 shows that project management leads, organises and controls the activities of the project.

Figure 1: 5 Phases of Project Management [smartsheet.com and PMBOK® Guide]

Project management is an integrated management control system helping the success of the whole of the innovation process (the project itself), which includes the whole life cycles of the project, from defining the problem to implementation [5]. Project management is an area focusing on the organization and control of resources. Its aim is to make sure the goals of the project are successfully achieved within a given framework of time and cost, as a result of the work performed by the resources [6]. Since projects are not repeated with the same conditions, it is not possible to create recipes for their implementation, only

efficient techniques that create results faster. Matching these techniques with the project is a specially important task of project management. Important characteristics of projects covered by project management:

- the task is a one-time task, not repeated (standard solutions cannot be used)
- the task is complex (it requires the coordination of the work of the given area)
- the task can be precisely identified (in terms of goals, performance criteria, and time, cost and resource requirements)

2.2 The phases of a project

For organisations, the greatest challenge besides everyday operation is the proper preparation and implementation of projects [7]. While the control and execution of normal business processes have been fine-tuned for a long time, projects are always unique, with different goals, problems and participants. Therefore, the efficient and successful implementation of a project requires sound and tested methodology and an expert who is skilled in it (the project leader) [5]. The project is the end product of the implementation process. I divide projects into three phases in my paper (see Fig. 2).

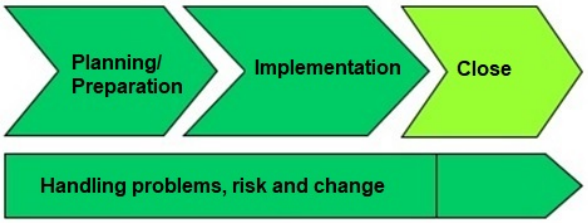

Figure 2: Typical development phases of an engineering project [Eszenyiné, 2014 and my own figure]

Planning phase: setting the goal(s), analysis of the situation and the problem(s), setting the parameters (money, time, human resource and material requirements), method of decision making and defining the roles. Its primary goal is to create a schedule of implementation of the project, which is basically a communication tool and incentive but also a tool of monitoring, and as such it must be able to handle any changes occurring during implementation. The most important methodological aspect of project planning is the selection of the form of planning matching the character of the project best (optimal form of planning).

Implementation (Execution) phase: Execution largely depends on preparation. Execution is successful if the work is characterized by transparency, flexibility and accuracy. The work is led by the project manager. The project manager leads the project, and is solely responsible for its execution, but especially for the performance parameters, costs and deadlines. Project management is leading, controlling and organising the execution of the project, and concentrating the resources, information and the methodological and technical tools for the purpose of reaching the goal(s) of the project. The tasks of project management can be documenting the project, collecting and transferring information, coordinating and organising the work, monitoring a deadlines and costs, obtaining permits, preparing and making decisions, checking the process, keeping in touch with partners, team building, and monitoring and evaluating internal and external feedback. The project manager always gets their decision making power from the top management of the company. The authority of the project manager largely depends on their ability to influence, which is greatly influenced by their management style, in addition to other factors, such as professional competence, negotiation skills etc. Based on their management style, managers can be task-oriented or people-oriented. A project manager must be able to strike a balance between the task-oriented approach and the people-oriented approach.

Closing (Evaluation) phase: The closing phase includes evaluation in addition to follow-up work. It means that it is determined whether the goals have been reached, and what is thought about the work by the people who took part in it and the people for whom the work was done. Evaluation includes examining the results and the process leading to them so that we can learn from the successes and mistakes made, and the conclusions drawn can be used in the next project. The project should not just be evaluated through some indicators but through the whole process. Project management interprets the success of the project in three dimensions. A successful project is one that is executed according to the original schedule, the original professional requirements and within the original budget. The goal of evaluation is to determine whether the execution of the project was successful:

- for the customer, the project is successful if it ensures reaching the customer's goal;
- for the entrepreneur, the conditions of successful execution are connected to technical and performance parameters and keeping within the schedule and budget.

It is important that in addition to the general condition of success, the process is analysed based on the individual criteria of success as well.

2.3 The financial and economic evaluation of a project

Project life cycle analysis: Generally, the starting point of a project is the concept, the idea, which is connected to an assignment, a customer need or perhaps a novel idea. Its end is the product in the general sense, which is created when the project is finished, and which constitutes economic benefit for both the customer and the project manager. The most general project life cycle is similar to the life cycle of a product. In Fig. 3, the horizontal axis shows time and the vertical axis shows the resources used in the project (man-hours money etc.), that is, the work invested into the project [8].

Economic analyses according to the life cycle principle: One type of the analysis of projects is based on the whole life cycle of the end result of the project (Fig. 4). The basic assumption is that the output of the project can be sold on the market or can at least be numerically quantified. The costs incurred in execution are offset by the revenue of selling the results on the market. If the product is not sold but e.g. a technological development resulting in savings, then the costs are offset by the savings. Economic analysis does not only take into account the life cycle of the project but also the life cycle of the final product of the project as well. Economic analysis is therefore carried out taking into account all effects of the project.

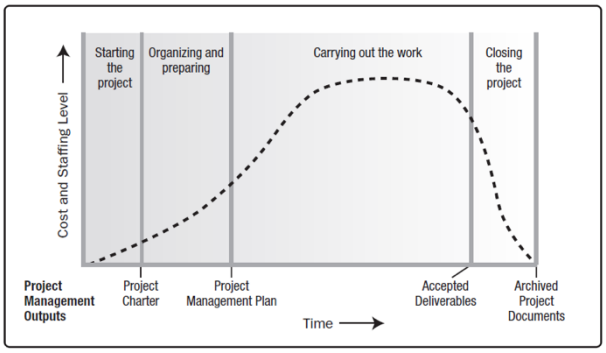

Figure 3: Life cycle phases of projects [karneliuk.com and PMBOK® Guide]

Fig. 4 shows how project life cycle and product cycle are related. Economic calculations made with Net Present Value (NPV), Internal Rate of Return (IRR) or the Profitability Index are to be made for the whole product life cycle [9]. In the case of product development projects, this principle has to be followed. Net present value shows the value of cash flows created during the term of the project (incomes and expenditures) discounted for the present. A project is worth executing if NPV>0. The higher this value is, the better the project is. The Internal Rate of Return (IRR) is the r value where NPV = 0. The higher IRR is, the more favourable the project is considered. This value is directly comparable in the case of projects of different sizes, where the created NPV does not reflect success. The Profitability Index compares Net Present Value with the investments made into the project. A project should be executed if the profitability index is higher than 1. If it is less than 1, it means that the returns are less than the investment. In another type of analysis, the effects of the end product are not considered, and analysis is only done for the life cycle of the project. Analysis is done this way when the effects of the end product cannot be taken into account (e.g. a project of organizational change) [10].

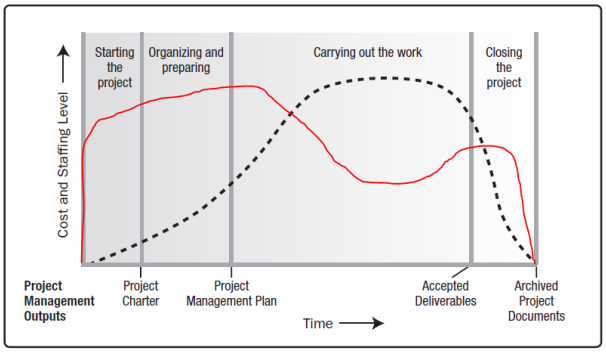

Figure 4: Economic analysis based on the life cycle of the project [karneliuk.com and PMBOK® Guide]

In certain cases, decisions have to be made based on qualitative, not quantitative considerations. In such cases aspects such as closeness to customers, communication skills, reaction speed etc. have to be taken into account. Economic analysis has to be made with the use of these aspects as well [11].

3 THE SUCCES FACTORS OF IT PROJECTS

Traditional project tools and methodologies (e.g. the Project Management Guidebook PMBOK® Guide) [12] [13], are necessary but not enough for the execution of IT projects. Such projects are complex and uncertain, and the success factors are difficult to measure). Standish Group International Inc., or Standish Group (http://standishgroup.com/) is an independent international IT consultant company founded in 1985 [14]. It is well-known for its IT projects in the public and the private sector. The company focuses on software applications of critical importance, with special attention to mistakes and the possible development of IT projects. Standish Group has been measuring the success of IT projects since 1994 [15], which has not changed much despite the numerous studies, books and methodologies published. Table 1 shows that in 2015 [16], 29% of IT projects were successful, 19% was not finished at all and in 52% one or more project conditions had to be changed (time, resources, expected result). The above mentioned survey can be criticized [17]. It is not clear what success means exactly in an IT project, and changes can also be beneficial. The "shocking" replies obtained from asking a large number of respondents, however, cannot be ignored as there have not been any other global surveys. An IT project—based on its result—selects, introduces or develops IT solutions or systems in line with the strategic goals of the organization.

Table 1: Success of IT projects [Standish Group, 2018 and my own table]

	1994	1996	1998	2000	2002	2004
Successful	16%	27%	26%	28%	34%	29%
Not finished	31%	40%	28%	23%	15%	18%
Changed during execution.*	53%	33%	46%	49%	51%	53%
	2006	2007	2008	2009	2010	2011
Successful	35%	35%	32%	32%	37%	29%
Not finished	19%	19%	24%	24%	21%	22%
Changed during execution.*	46%	46%	44%	44%	42%	49%
	2012	2013	2014	2015		
Successful	27%	31%	28%	29%		
Not finished	17%	19%	17%	19%		
Changed during execution.*	56%	50%	55%	52%		

* the project exceeds its cost or resource limits, or is not executed according to the plan.

The project management triangle (Fig. 5) is sometimes called Iron Triangle or Triple Constraint. It means that if the budget, schedule or scope of a project is changed, it affects one or two of the other elements. A project is always balancing between the vertices of the project triangle. The three factors usually work against each other. The task of

the project manager is to save the project triangle from collapsing.

Figure 5: The project triangle [t2s-solutions.com]

Traditional project management measures the success of projects with the realization of the iron triangle (resources used – time – scope = quality). In the case of IT projects, however, far more—usually difficult to measure—success factors have to be taken into account [6]. The fourth element of the project triangle, quality, is in the centre—modifying any side of the triangle changes it. It is very important to note that quality does not have a universal standard. Quality must always be defined within the project itself. There are companies which focus on keeping within the budget in defining project success. For others, finishing the project quickly is more important. The project manager must know the exact definition of success in the case of the given organization and project.

Figure 6: An extended interpretation of the success factors of projects [Deák, 2005 and my own figure]

The most important task of the project manager is to make the project successful. Very often, however, in managing projects, companies face failure instead of success. Nowadays, however, failure is not only a characteristic of unusual, unique projects. Project success is of primary importance from the point of view of project management since without project success, companies cannot reach their strategic goals or realize their incomes. Much research has been done into project success, resulting in different approaches. It is important that failure can rarely be explained with the lack of resources as these are available on the market almost without limit. Far more important are qualitative factors such as insufficient definition of project area or a lack of project management knowledge (see Standish Group reports). The efficiency of project management shows how well the project has reached its goals on the one hand, and how much it has contributed to the goals of the organisation on the other [18]. Fig. 5 shows that the quality – cost – time triangle can indicate the results of the project but this is only part of the success of the project. Comprehensive assessment also includes compliance with strategy and the satisfaction of stakeholders as well. The project triangle is still the most widely used method of measuring success. However, even the interpretation of success is not uniform. According to the literature [19], there are two approaches to quality: the general philosophical interpretation and the value-based philosophical interpretation. In the case of projects won in tenders, the two defined categories can also be spotted in the interpretation of success [20]:

- in the general philosophical interpretation of a project, an activity or its results can be described well with the various indicators and the outputs prescribed and expected in the given program and planned in the submitted application;
- the value-based philosophical interpretation can be used both for the assessment of projects won in a tender and the evaluation of the utility of executed projects, because the emphasis on the usefulness for the different target groups is great.

4 Information security training project

Nowadays, information security, the protection of the data of offices, companies, and private persons is gaining paramount importance. Unauthorized access to data whether by accident or intentionally, and stealing or malicious manipulation of data causes considerable damage to the affected parties; their reputation is damaged and trust in the service is lost [21] [22]. Also, the incorrect handling of data can lead to legal consequences (e.g. GDPR) [23] and damages. International data shows that loss of data and unauthorized access to data can most often traced back to human error—with more attention from the employees and by complying with the rules the incident could very often have been avoided. According to paragraph 11, section (1) c) of the Act No. L. of 2013 [24]. on the Electronic Information Security of Central and Local Government Agencies (information security law) the leader of the organization appoints a person responsible for the security of the electronic information system, based on the requirements provided by security class of the electronic information system and the security level of the organization. The training and in-service training prescribed by the information security law is included in detail in the 26/2013. (X. 21.) KIM decree [25]. The information security law contains the rules applying to the security and protection of data that is part of the national wealth. The law contains many conditions for protection, one important element being the security awareness training of the users. The execution decree of the law, BM decree 41/2015. (VII.15.) [26] states that the organization organizes security awareness training of the basic security requirements for the users of the electronic information system, to prepare them to recognize possible internal threats. Training should not only be provided once, when the employee is hired, but regularly (ideally annually) to update and refresh the knowledge of the users.

4.1 Targeted attacks on public administration

With Targeted Attacks, attackers target a particular target (person or organization). As opposed to a computer virus, the "creator" of the threat does not seek to spread the malicious code as widely as possible, but to install it into the target's devices. Targeted attack tools are a combination of simpler attacks (web attacks, letter attacks, system attacks etc.) that call for very great expertise, because these devices and systems are usually well protected [27].

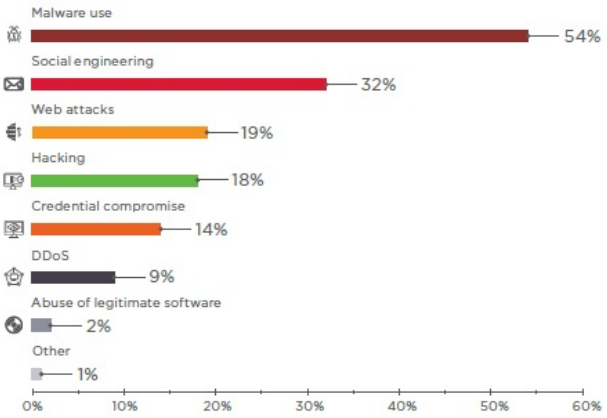

Figure 7: Government: attack methods used in 2018 [Positive Technologies, 2019]

Advanced Persistent Threat (APT) attacks require a great deal of expertise—they are executed by highly skilled professionals who are mostly employed by state intelligence services or criminal organizations to obtain data or information about a system or sector (Leitold, 2014). APT attacks are different from traditional cyberattacks in their choice of target, their duration of attack and length of incubation period. Fig. 7 shows that these attacks exploit targeted psychological manipulation (Social Engineering) attacks [28]. In recent years, targeted attacks have been on the rise, and this year (2019) will not be an exception either [29].

CONTENTS

Figure 8: The contents of the professional material [my own figure, 2018]

4.2 IT security awareness training

Organizing information security training and in-service training is mostly the responsibility of the National University of Public Service (NKE). The training of organisational leaders, experts, contributors and workers started based on the information security law passed in 2013. So far NKE has trained about 150 people. The task of the Cybersecurity Academy started in March 2017 is to coordinate the existing resources of the faculties, research institutes and workshops, and support cybersecurity research and experts. They start and organize training programs and plan cybersecurity practices. The goal of the academy is to serve as a catalyst in cybersecurity training in the areas of public service, law enforcement and national defence [30].

4.3 Information security in-service training

The European Commission in its C(2015) 5262 decree approved the Public Administration and Public Service Development Operative Program (KÖFOP), and the government determined the annual budget of the KÖFOP in the government decree 1004/2016 (I. 18.). In its Appendix 2, it designated the project "The technological development of public service complex competence career program and education" project with the ID number KOFOP-2.1.1-VEKOP-15-2016-00001 as a project of outstanding importance. I took part in the preparation of the professional material connected to the "Annual in-service training for the person responsible for the security of the electronic information system – targeted cyberattacks" (50 hours) training program, which is part of the project [30]. The professional material entitled "Targeted attack against the public administration sector" was prepared by March 30, 2018. It is a Hungarian language 20-page material. Fig. 8 shows the contents of the document, which can be later downloaded as e-learning teaching material from the website of the Faculty of Political Science and Administration, Leadership and Training Center Specialist Training Department of the National University of Public Service.

Table 2: Phases of preparing the professional material (my own compilation, 2018)

Phases of the project	Milestones	Tasks accomplished	Notes
Signing the contract	28.12.2017	The user commissions the author	Determining the requirements of the project
Planning and preparation	29.12.2017–11.01.2018	Making the interview questions	The structure of the professional material, creating the chapter titles
Execution	12.01.2018	Making the interviews with the four professional leaders	Taking into account the information security trends
	13.01.2018		
	16.01.2018		
	17.02.2018		
	18.02.2018–15.03.2018	Processing the literature connected to the topic	
Closure	15.03.2018–30.03.2018	Finalizing the professional material, proofreading and submitting it	According to the conditions laid down in the contract

5 CONCLUSIONS

Nowadays, public organizations must give priority to providing information security while ensuring their day-to-day business, as the preservation, integrity and availability

of confidential information is essential. Information security is now seen not only as prevention, but also as a comprehensive strategic issue. Companies often attempt to cover information security tasks by creating IT security, but this is not a one-off task, but a result of a complex, multi-player process. IT security is thus increasingly becoming a business continuity issue for both companies and public services. For this reason, an appropriate IT security approach is increasingly a proactive approach: a careful assessment of security options and risks, an appropriate level of empowerment of users and ongoing training—some of the most important measures that need to be taken to ensure effective IT security.

The professional material was finished and the information security training project was successful. It was successful because the phases of the project and the milestones were finished in time and the conditions laid down in the contract were fulfilled. Each chapter started with a literature review and the theoretical background, and continues with the interviews with the leaders, turning theory into practice applicable in day-to-day work. The project was financed by the European Social Fund and Széchenyi 2020. 80.9% of the costs of the project is covered by the convergence (KÖFOP) source and 19.1% from the Competitive Central Hungary Operational Programme (VEKOP), considering that the defined tasks are connected to the project with the ID KÖFOP- 2.1.1-VEKOP-15-2016-00001.

REFERENCES

[1] Zs. Szabó (2017): The Information Security and IT Security Questions of Pension Payment. In: Lucia Figuli, Pavel Manas, Alexander N Kravcov, Václav Pospíchal, Bohuš Leitner, Pavel Svoboda (editor) Structural and Mechanical Engineering for Security and Prevention: ICSMESP 2017. Prague, Czech Republic. 2017.06.14-2017.06.16. Prague: Trans Tech Publications. 2017. pp. 322-327.

[2] P. Michelberger, Cs. Lábodi (2012): After Information Security - Before a Paradigm Change: A complex Enterprise Security Model. Acta Polytechnica Hungarica 9:(4). pp. 101-116.

[3] Michelberger, P. (2015): Információtechnológiai projektek másképpen, HADMÉRNÖK 10:(1) pp. 224-233.

[4] Henczi, L., Murvai, L. (2012): Projekttervezés és projektmenedzsment, Saldo Kiadó, Budapest. pp. 1-184.

[5] Verzuh, E. (2006): Projektmenedzsment, HVG könyvek, Budapest. pp. 1-424

[6] Dennis, L. (2007) Project Management (9th ed.) Gower Publishing, Ltd.. pp. 1-545.

[7] Eszenyiné, B. M. (2014): Projektmenedzsment a könyvtárban, Debreceni Egyetemi Kiadó. pp. 1-95

[8] Daróczi, M. (2011): Projektmenedzsment, Szent István Egyetem, pp. 1-152.

[9] Csiszárik-Kocsir, Á. (2018): Vállalkozások pénzügyei, Óbudai Egyetem, Budapest. pp. 1-192

[10] Bucsy L. (1976): Az innovációk rendszere és a vállalati fejlődés. Közgazdasági és Jogi K Budapest. pp. 31-41.

[11] Á. Csiszárik - Kocsir, J. Varga, Crisis (2017): Project - Risk: According to the Opinions of Hungarian SMES, Project Management Development - Practice and Perspectives: Sixth International Scientific Conference on Project Management in the Baltic Countries. pp. 60-70.

[12] Project Management Institute (2013): A Guide to the Project Management Body of Knowledge (PMBOK® Guide), 5th Edition, pp. 1-589.

[13] Project Management Institute (2017): A Guide to the Project Management Body of Knowledge (PMBOK® Guide), 6th Edition, pp. 1-573.

[14] Standish Group International Inc. (1994): CHAOS MANIFESTO. https://www.standishgroup.com/sample_research_files/chaos_report_1994.pdf (Downloaded: 20/11/2018)

[15] Standish Group International Inc. (2013): CHAOS MANIFESTO. http://www.versionone.com/assets/img/files/CHAOSManifesto2013.pdf (Downloaded: 21/11/2018)

[16] Standish Group International Inc. (2014): CHAOS MANIFESTO. https://www.projectsmart.co.uk/white-papers/chaos-report.pdf (Downloaded: 22/11/2018)

[17] Eveleens J. L., Verhoef, C. (2010): The Rise and Fall of the Chaos Report Figures. IEEE Software. Vol. 27. No.1. pp. 30-36.

[18] Deák, Cs. (2005): Projekt menedzsment képességek szervezeti szintű fejlesztése, „Tudásalapú társadalom Tudásteremtés - Tudástranszfer Értékrendváltás." V. Nemzetközi konferencia, Miskolci Egyetem Gazdaságtudományi Kar. II. köt. Miskolc-Lillafüred 2005. május 11-12. pp. 80-86

[19] Veress G. szerk. (1999): A minőségügy alapjai, Műszaki Könyvkiadó, Budapest. pp. 1-281

[20] Veress, G., Birher, N., Nyilas, M. (2005): A minőségbiztosítás filozófiája. JEL Könyvkiadó, Budapest. pp. 1-281

[21] T. Szádeczky (2015): Information Security Law and Strategy in Hungary, Academic and Applied Research in Public Management Science 14:(4). pp. 281-289.

[22] Z Rajnai, B. Puskas (2015): Requirements of the Installation of the Critical Informational Infrastructure and its Management, Interdisciplinary Description of Complex Systems 13: (1) pp. 48-56.

[23] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN (Downloaded: 17/11/2018)

[24] State and Local Government Bodies Act L of 2013 on the Security of Electronic Information Systems. Hungarian Gazette No. 68 of 2013 pp. 50241-50255.

[25] 41/2015. (VII. 15.) BM on the requirements for technological security as well as the requirements for safe information tools, products, safety class and security classification as defined in Act L of 2013 on Electronic Information Security of State and Local Government Bodies, Hungarian Gazette 2015 # 103. pp. 17700-17751.

[26] 26/2013. (X. 21.) KIM Decree on the security of the management and electronic information system specified in the Act on the Electronic Information Security of State and Local Government Bodies, Magyar Közlöny 2013, No. 173. pp. 74208-74212.

[27] Zs. Szabó (2017): Cybersecurity issues of pension payments. In: Szakál Anikó (szerk.). IEEE 15th International Symposium on Intelligent Systems and Informatics: SISY 2017. Subotica, Serbia. 2017.09.14-2017.09.16. New York: IEEE. pp. 289-292.

[28] Positive Technologies (2019): Cybersecurity threatscape 2018: Trends and forecasts. Cybersecurity_threatscape-2018-Q4_A4.ENG.0002.03. pp. 1-22. https://www.ptsecurity.com/upload/corporate/ww-en/analytics/Cybersecurity-threatscape-2018-eng.pdf (Downloaded: 07/05/2019)

[29] Zsolt, Sz. (2018): Cybersecurity issues in industrial control systems. Anikó, Szakál (szerk.) IEEE 16th International Symposium on Intelligent Systems and Informatics: SISY 2018. Budapest, Magyarország: IEEE Hungary Section, 2018. pp. 231-234.

[30] Szabó, Zs. M. (2018): Célzott támadás a közigazgatási szektor ellen. Deák, Veronika (szerk.) Célzott kibertámadások: Éves továbbképzés az elektronikus információs rendszer biztonságáért felelős személy számára 2018. BUDAPEST: Nemzeti Közszolgálati Egyetem. pp. 156-167. http://m.ludita.uni-nke.hu/repozitorium/handle/11410/11181?fbclid=IwAR1WcvyF1eD9K-u0HkKUmzmGrRwtA1etfwoAiqAPloG77HzPZQReKtSA4V8 (Downloaded: 21/11/2018)