Volume 4, Issue 9, September 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Security Challenges in the Use of New Technologies in Public Administration

[1]Milica Tepsic, Ph D, [2]Mladen Radivojevic, Ph D, [3]Dijana Tepsic, MA

[1]Ministry of Administration and Local Self-Government, Banja Luka, Republic of Srpska, BiH, Bosnia and Herzegovina

[2]University for Business Studies, Banja Luka, Republic of Srpska, BiH, Bosnia and Herzegovina

[3]Gender center – Center for Gender Equality, Banja Luka, Republic of Srpska, BiH, Bosnia and Herzegovina

Abstract— Computers and other information and communication technologies (ICT) are increasingly taking over and most vital function of human activity, including public administration. A public administration provides to the citizens of crucial importance for the quality of their lives. The data and information that the public administration has always had a very great importance and therefore, at the time of the reform of public administration and its transformation to e-government (e-government), it is necessary to offer complex solutions concerning their protection and safety. This paper should contribute to improving information security in general, and particularly in public administration as well as comprehensive information security open issues in public administration.

Keywords— - information security, public administration, information and communication technology

I. INTRODUCTION

The current mode of public administration, organization and legal framework can not provide the required efficiency or quality of its service. Given that ICT represents a generator of change and based on the development of modern societies and economies in the XXI century, improving efficiency and quality of public administration through the use of ICT would significantly affect the overall trends, economic prosperity and every other society in which we live. With the development of technology developed and better security technologies, which make it difficult finding a technical failure. Therefore, attackers are increasingly turning to the human factor, and are very important in public administration officials to raise awareness about the need for information security. It turned out that the provision of the information system using standard security products - firewalls, intrusion detection systems, or devices to identify longer enough. Therefore, it is necessary to point out the role of the consciousness of the need to achieve information security, which is reflected in the safe use of ICT, secure electronic commerce, protected communication, guaranteeing privacy and dr.

Many studies show that a person is a key factor in information security. He is the creator, the holder, the user and the cause of theft, damage or destruction of information, because it creates, creates and implements information security, but (unfortunately) on the distort [1].

A very important factor is the physical security of the system, and may endanger the natural disasters such as fire, flood, lightning or earthquake threats from the environment, such as heating, cooling and electricity, as well as the users of the system or who do not have access to the system.

II. IMPACT OF INFORMATION AND COMMUNICATION TECHNOLOGY IN OPERATION OF PUBLIC ADMINISTRATION

The time in which we live is an intense phase of the development and application of new technologies. Computers, unique in their characteristics and capabilities, as well as the Internet, Web technology and business intelligence, increasingly enters our life and the way of life and work. The great importance of new technologies in their ability to liberate man from fatigue, simple, and very exhausting work, and to strengthen the power of his mind. Of new technologies, management information systems, knowledge management is becoming a very important discipline [2].

According to some research, all human knowledge accumulated until the twentieth century doubled its first half. Until next doubling took place, but after ten years, and it is assumed that at the present time it happens every five years. Measure the amount of knowledge can be the amount of information, and no new scientific approaches, new methods and new technologies can not control the amount of information. At this point, mention should be made of so-called "Moore's" law. According to this law the number of transistors that can be placed on an integrated chip doubles every 18 months. On the other hand, the silicon semiconductor technology will reach the physical limits for the next 10 to 20 years. The future, in this sense, has already begun. Therefore, around 2020, Moore's Law will cease to be valid because the size of electronic circuits to achieve the dimensions of atoms and molecules. The technology is basically the so-called quantum computers, which in recent years have developed. A quantum computer uses the direction of atomic spin to represent zeros and ones - cubits - unlike electrical charges that are used in silicon computers.

Many computer systems today are networked in some way, most of the global computer network Internet, which is easier and faster everyday work, and especially prominent, speed and ease of communication with others via the Internet.

[3] New figures released today by ITU indicate that, by end 2014, there will be almost 3 billion Internet users, two-thirds of them coming from the developing world, and that the number of mobile-broadband subscriptions will reach 2.3 billion globally. Fifty-five per cent of these subscriptions are expected to be in the developing world.

"The ICT Newly released figures confirm once again that information and communication technologies continue to be the key drivers of the information society," said ITU Secretary-General Hamadoun I. Touré.

"If we want to understand the information society, we have to measure it," Brahim Sano the Director of ITU's Telecommunication Development Bureau, said. "Without measurement we can not track progress or identify gaps which require our attention."

The Internet is a cyber world that can cruise from continent to continent in a very short time [4], beyond the limits of space and time, allowing almost instantaneous, timeless (timeless time), transfer of information, thus overcome the problem of physical abilities and limitations of man, to overcome seemingly insurmountable barriers of space and time it is facing. ICT has enabled everything works faster, easier, cheaper and better, changing completely the way in which man interacts, learns and works.

Theoretically, we are able to convey our computer millions of pages of text on the topics that interest us and interact with thousands of people who have similar interests as me. The latest trend is toward embedding computing capabilities in all types of devices used, and thereby the dependence on computers has become total or close to total [5].

It is expected that the rapid development of information system resources and continue. This primarily refers to the hardware, software and databases. Here are just facts: 50 years ago on one computer came around 300,000 users. Than thirty years ago a computer can use one user. Now the situation is such that a user via the Internet using thousands of computers and computer networks.

There are several studies on the development of the information society in the world, using different indicators. Thus, for example, The World Economic Forum takes into account three groups of factors: the index of the environment (market, political, legislative and infrastructure) Readiness Index (individual readiness, business and government), and the index of use (individual use, business and government use).

In the latest report by the World Economic Forum on the use of IT in the 2013, countries in the region are placed in the following order: Slovenia at the 37, Croatia is 51, Montenegro 48, Macedonia FYR 67, Bosnia and Herzegovina 78 and Serbia 87, on the list of 148 countries. Leading positions occupied by Finland, Singapore, Sweden, Netherlands and Norway, while Myanmar, Burundi and Chad are at the end of the list.

Bosnia and Herzegovina for the first time appeared in the report of the World Economic Forum (WEF) in 2004-2005. In this report, BiH has taken 89 places out of 104 countries. In the series of these statements in the period since 2004 by 2009, shows that BH had a lot slower grow than other countries in the world and in the region. Of particular concern is the slow development of e-government readiness, where BiH was 87 in 2004, out of 104 countries, and in 2006 was 104 out of 122 countries, in 2009 in 129 place out of 133 countries, so at the very bottom of the list. The report of the 2004 / 2005 based on the individual readiness of BiH on 77 places out of 104 countries, and in 2009 on 63 out of 133 countries included in the report. These results suggest that BH has a good basic infrastructure for the development of ICT, and individuals are using it, and the institutions of government and business actors are far behind them. This certainly contributes to a very bad market, political and regulatory environment; making Bosnia and Herzegovina at the bottom of e-readiness of countries included in the WEF surveys (see Table 1, below).

The following table summarizes the results of the WEF in Bosnia and Herzegovina in the period of eight years.

Table 1
Ranking of BiH to the e-readiness indicators (WEF, The Global Information Technology report) [6]

	2004/ 2005	**2005/ 2006**	**2006/ 2007**	**2007/ 2008**	**2008/ 2009**	**2009/ 2010**	**2010/ 2011**	**2011/ 2012**	**2012/ 2013**
Number of countries (N)	**104**	**115**	**122**	**127**	**134**	**133**	**138**	**142**	**144**
Networked Readiness Index	89	99	89	95	106	110	110	84	78

If we compare Bosnia and Herzegovina with the countries of the former Yugoslavia, then we see that B & H significantly lags behind other countries in the region (see Table 2).

Table 2
Ranking of countries in the region, according to the WEF

Country	2009/10	2010/11	2011/12	2012/13
Slovenia	31	34	37	37
Montenegro	42	44	46	48
Croatia	51	54	45	51
Macedonia	73	72	66	67
Serbia	84	93	85	87
Bosnia and Herzegovina	110	110	84	78
Total state	133	138	142	144

He's unstoppable trend of globalization, the pace of business change is more pronounced, increasing the number of innovations, the environment in the narrow and broad sense changes, the requirements for more efficient and cheaper administration and services are increasing. Public administration uses new technology to be more efficient, more reliable and cheaper, more oriented towards citizens, and that citizens provided a simpler and faster access to information and services, and that her work is more accessible to the public eye. Application of new methods of management and the introduction of modern technologies in the administration increasingly weak control, and strengthen the service management function.

Unlike traditional public administration, e-Government is a phenomenon that is under development, because it means fully perform administrative tasks electronically without using paper. The term "Government" has no single definition, and its meaning has different interpretations in different cultures. In the United States, under this term refers to the total power, which includes all the columns and levels of government. In Britain, as in France ("Government") and Germany ("Regierung"), under the term refers to the executive branch, while in the U.S. for this concept uses the term "administration" or administration. Here the term is used as a "public authority", or "electronic public administration," referring primarily, but not exclusively, to the executive, as it has traditionally been a key place in the public service. The transformation of public administration in e-government will allow public administration from the traditional hierarchical and bureaucratic model is transformed into a dynamic model of networked governance (networking governance). Therefore, public administration must implement the transformation of their internal processes, and the environment, particularly with regard to the introduction of e-services, knowledge management and interoperability of different applications, then security environment, the bandwidth of the Internet and the introduction of e-commerce and digital signatures. The development of e-government based on the use of ICT to increase the quality of services by the government, providing quality information to citizens and businesses, as well as more efficient and transparent operations. Thus, e-government can be viewed from the "on-line access to services" to "tools for the construction and restoration of democracy". [7]

E-Government operates on the principle of "3B" (anything, anytime and anywhere), that is, users of government services may at any time, for any need from any place to turn to government. In communications science of new media this model is known as the AAA paradigm of large telecom operators: anything (anything), anytime (anytime), anywhere (anywhere). For Francis Balle it is "the ultimate achievement, omega principle communication society ..." [8]. Public administration acting on these principles is fully and permanently operational and assumes the integration of information systems and subsystems. The documents of the countries in transition to e-government as the main reason for its introduction states striving to: provide a new foundation for economic competitiveness; allow the redefinition of the role and quickly perform the transformation of government and administration, and converting them into service for the citizens; reducing the cost of public services; to boost the development of knowledge-based economy; integration; facilitates the use of public services; define better policies and improve and accelerate the decision-making process; as well as to ensure the efficiency and effectiveness of government at all levels.

New technologies and quality regulations may provide for improved communication, both within the public administration and in its environment, hence better cooperation between public administration, citizens and business systems (G2B, G2C and B2G model). Harmonization of regulations with opportunities to apply information and communication technology and business intelligence can make public administration more efficient, thus Ensuring customer satisfaction of public services.

III. RISKS AND HAZARDS OF ELECTRONIC BANKING IN PUBLIC ADMINISTRATION

The introduction of the Internet for the global community was soon revealed an indisputable fact that it is crowded with risks associated to undesirable elements eager, willing and able to abuse its capabilities. Besides creating huge social and economic opportunities, boundless and anonymous nature of the Internet is a huge challenge. Information technology makes it an ideal platform for penetration into other people's computer systems, and also carry a variety of criminal activities. Criminals exploit this same technology to carry out criminal acts and violate the security and privacy of users of IT. In the hands of persons who act dishonestly, maliciously or recklessly, this technology becomes a tool for activities that threaten lives, property, and dignity of individuals and harm the public interest. Indeed, more people going to the network, the more criminals realize that online crime can be very lucrative, especially considering the amount of valuable commercial and personal information now housed in electronic form [9].

State administrations, organizations and entire society depend to a high degree of efficiency and safety of modern information technology. International Computer networks are the nerves of the economy, the public sector and society as a whole. Information infrastructure has become a critical part of the backbone of the economy. Safety of the computer and communications systems and their protection from abuse are therefore essential. The spread of information technology in almost all spheres of life, as well as connecting computers to the international computer networks have contributed to criminal activities become more diverse, more dangerous and with international presence [10].

Multiplied dependence on technology conditional on the risks and dangers of business that uses this technology. The fact is that the more information we produce, the greater is the importance of the security of such information. If thirty years ago disintegration of information system was just a small inconvenience, today, in some systems, would be a disaster. Therefore, with each new achievement in the sphere of information technologies emerge new aspects of information security.

Those familiar with historical trends know that in the history of the development of mankind, nothing has developed so quickly and had a greater impact on all changes in human society than information technology. Unfortunately, such a big change, carry with them the risk of unintended consequences that inevitably stem from these turbulent processes. Therefore, particular concern is the fact that they may become dominant in relation to the desired state.

So great challenges require adequate answers. So to answer the question whether a man will in the near future, be able to control with mind what is made by hand (?) - Information technology - determine the contours of the events in which there will be quite clear whether the man "of his servants made lord"?[1]

Anthony Giddens shows that the world we live in today does not look as it is anticipated, that we are increasingly getting out of control and concludes that we will never be masters of our own history, but that we can and must find ways not to deliver this "runaway world " to Hell [11].

Cloud computing also brings a large number of issues related to data security. Regardless of the type of user, all are concerned about data security in the cloud and in the protection of privacy. Of course that these issues and concerns are justified especially at a time when we know for cases "WikiLeaks" and "Snowden" but on the other hand we should kept in mind that these cases, as well as many others, are related to the "eighth layer of the OSI". In case you are wondering who the eighth OSI level is, the answer is MAN. Security in the Cloud should be seen from two aspects, the first is the technical aspect where we talk about technological solutions and the other aspect is the legal regulations relating to standards and legal framework that will provide security within the legal framework. The boundaries of information systems have disappeared, and the availability of the system is possible from every point of the world and from all types of devices. Mobility and availability of information has experienced expansion in recent years and the economy has made cloud computing wide accepted [12].

Public administration is working with very important information about citizens and economic entities and therefore its responsibility is even more to protect them from loss (destruction), swelling (downloading, copying, interception), deformity (modification, falsification) or blocking.

No matter in what form are stored, transmitted and used, information must be adequately protected. To ensure adequate protection of information, all users must be familiar with the concept and the measures of protection required. The protection of information, preservation of the confidentiality, integrity and availability, it becomes of prime importance. Problems that the public administration is facing when it comes to current trends in the use of new technologies, when employees use mobile devices, cloud computing, operating in the virtual environment, are new types of risk and it is necessary to quickly respond to these problems. Is necessary to define the requirements for safety, choose and install controls, to ensure that risks are reduced to an acceptable level.

One of the key slogans of safety information is: "Prevention is ideal but detection is an obligation" [13].

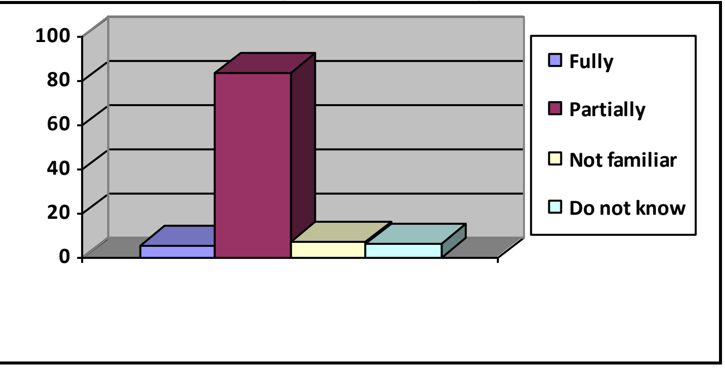
IV. EMPIRICAL RESEARCH

The aim of this study was to evaluate the state of information security and the security of information systems in the public administration of the Republic of Srpska, and how much attention is paid to this very important issue, as well as to point to what should be done to improve the informational security. The study used more scientific research methods: analysis and synthesis, inductive-deductive, historical methods, comparative and statistical methods. The empirical method was dominated by content analysis and test methods. Empirical research has shown that the level of information security in the public administration of the Republic of Srpska is relatively satisfactory. All results obtained by empirical research are presented in tables and graphs, and this paper presents only a part of the research. In reaching conclusions about the research all the indicators and effects were taken into account. Analysis of the mean values and standard deviations showed the greatest deviation in protecting computer networks, and that also indicate the result of the correlation.

These data lead us to conclude that the improvement in the level of protection of the network infrastructure reduces the risk of compromising information security. As these data are very high statistical significance with certainty of 99%, we can argue that the re-investigation would come to the same data.

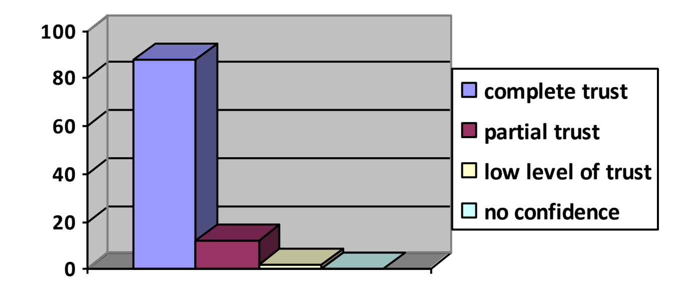
Further analysis of the results, and using the chi-square tests led to the information that results in the field of information security assessment and security of information systems (physical protection measures, protection systems, applications and databases, access control information system and the protection of computer networks) are reliable and significant. T test showed that the research in the field of information protection and protection of information systems provided adequate results and that we can safely say that new research would get the same survey data.

How many employees are familiar with the authorities in case of disaster	Number of respondents	
	F	%
Fully	5	4,90
Partially	84	82,40
Not familiar	7	6,90
Do not know	6	5,90
Total	102	100,00



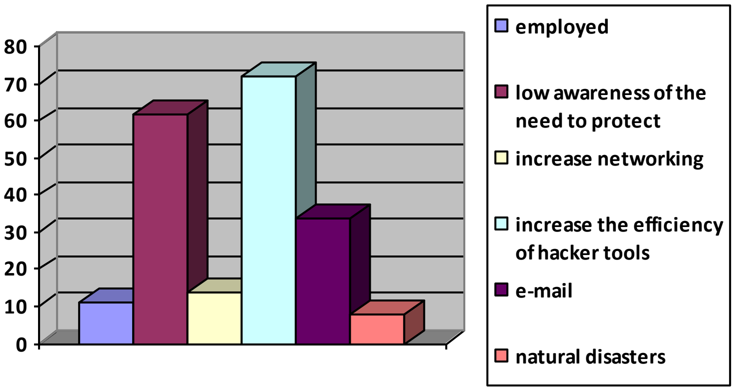
The table and chart no. 1: Distribution of institutions with regard to how employees are familiar with the powers and duties in the event of a disaster

The level of trust in the security of information systems	Number of respondents	
	F	%
complete trust	88	86,27
partial trust	12	11,76
low level of trust	2	1,96
no confidence	0	0,00
Total	102	100



The table and chart no. 2: Distribution of institutions with respect to the level of confidence in the security of information systems

The biggest threat to information system replies	Number of respondents
	F
employed	11
low awareness of the need to protect	62
increase networking	14
increase the efficiency of hacker tools	72
e-*mail*	34
natural disasters	8



The table and chart no. 3: Distribution of institutions given the level of threat information system

IV. CONCLUSIONS

Technique and technology can not replace, but can significantly facilitate the organization and implementation of information security. The focus must be on safety: prevention (through developing awareness of the dangers), training people (to recognize them, neutralize or reduce risks); to screen people and defining rules of safety behaviour; constant review of identified hazards and risks of their origin and development of usable and keeping up to date plans for risk mitigation and elimination of consequences.

No system is not fully perfected, each has some weak points and the absolute security of information system does not exist. In fact it is the absolute only for those systems – that does not exist [14]. Therefore, the goal of the security of information systems in general, including in electronic administration, is that the user is constantly confronted with potential hazards, risk is managed in the work of information systems, or to identify, control and minimizes or eliminates the security risk, which may have an impact on information systems, at an affordable price.

Theoretical and empirical analysis is confirmed, and the studies quoted in this paper suggest that without the protection and security of information and information systems in public administration does not have its safe functioning.

ACKNOWLEDGMENT

Thank you to everyone who participated and contributed to this study.

REFERENCES

[1] M. Tepsic: *Some aspects of information security in the system of public administration in the Republic of Srpska*, "News," Journal of Social Issues., UDC 351.9 [005:004 (497.6RS), Banja Luka, Bosnia and Herzegovina, 2010th.

[2] M.Radivojevic, M.Tepsic and B. Dumonjic: *Business Intelligence*, parable, and BLC, Banja Luka, 2011, ISBN 978-99938-1-148-0

[3] The latest ITU statistics are available at www.itu.int/en/ITU-D/statistics.

[4] Kent, P.: *Guide to the Internet (10 minutes to success).* Sign, Zagreb, in 1994.

[5] Cybersecurity Today and Tomorrow: *Pay Now or Pay Later*, National Academy of Sciences, National Research Council, Washington, D.C., ISBN: 0-309-08312-5, 2002, 50 pages, str. 2-3.

[6] http://www.weforum.org/reports/global-information-technology-report-2013

[7] Pedro G. Gonnnet: *The Future of Informatics as Scientific Discipline*, UPGRADE The European Online Magazine for the IT Professional, (http://www.upgrade-cepis.org), Vol II, No.4, August 2001.

[8] Francis Ball, *The power of the media*, Clio, Belgrade, in 1997.

[9] Crime online: *Cybercrime and illegal innovation*, Research report: July 2009, http://eprints.brighton.ac.uk/5800/01/Crime_Online.pdf

[10] R. Slobodan Perovic: *Knowledge against misuse of knowledge*, Proceedings "ZITEH 2010"

[11] Giddens A., *Runaway world*, Routledge, 2003, str. 2-5.

[12] Sasha Milasinovic, *Cloud Security - Challenges and Future,* Proceedings "ZITEH 2014"

[13] Dzigurski Ozren, *APPLICATION OF THE HONEYPOT ARCHITECTURE IN VULNERABILITY ANALYSIS OF INFORMATION SYSTEMS*, University of Belgrade, Faculty of Security Studies, Journal "ZITEH 2014”

[14] Rodić, B., Đorđević, G.: *Da li ste sigurni da ste bezbedni*, Produktivnost, Beograd, 2004