INFO- 2101
Primljeno/Received: 2013-04-18
UDK: 681.3:340:001
Authors Review/Pregledni rad

ICT AND IDENTITY THEFT

ICT I KRAĐA IDENTITETA

Krunoslav Antoliš

Police College, Police Academy, Ministry of the Interior of the Republic of Croatia, Zagreb, Croatia
Policijska akademija, Ministarstvo unutarnjih poslova Republike Hrvatske, Zagreb, Hrvatska

Abstract

Modern information and communication technology, apart from their numerous advantages, bring with themselves new forms of threats and dangers to which any of their users are exposed. One of the most serious is the identity theft through ICT which is the matter of concern not only for the victims but also for the experts in IT and legislation. This paper analyses technological and legal aspect of identity theft. Concerning technological aspect, the paper recognizes the manners of identity theft through ICT and the methods and techniques which ICT users can apply as their protection. With regard to legal aspect the paper examines the possibilities for protection within the existing legal framework and points out the possibility of its advancement by analyzing the experience obtained worldwide. All mentioned in the paper is aimed at protecting of the ICT users and also at creating preconditions for criminal proceedings of identity thieves.

Sažetak

Nove informacijsko komunikacijske tehnologije pored niza prednosti donose i nove oblike ugroza i prijetnji kojima smo izloženi prilikom njihove uporabe. Jedna od najvećih, koja pored žrtava uvelike brine informacijske ali i pravne stručnjake je krađa identiteta putem ICT. U radu se raščlanjuje tehnologijski i pravni aspet krađe identiteta. U tehnologijskom smislu važno u radu se prepoznaju načini krađe identiteta putem ICT te metode i tehnike putem kojih se možemo kao korisnici ICT zaštititi. U pravnom pogledu u radu se sagledava mogućnosti zaštite koje nam nudi postojeći zakonski okvir, a potom se raščlambom svjetskih iskustava ukazuje na mogućnosti njegova unapređenja. Sve radom spomenuto u funkcije zaštite ICT korisnika, ali i stvaranja preuvijeta za kazneni progon kradljivaca identiteta.

1 Introduction

Identity theft is a criminal offence which in recent years has inflicted millions of dollars damage to physical and legal persons, while dark figures, according to the experts, exceed billions of dollars at global level. Numerous examples illustrate that identity thieves recognized ICT as extremely vulnerable technology exploiting its vulnerability for criminal profiteering applying various technical tools (hardware/software) for identity theft and fraud as well as social engineering methods. In the world of global communications, Skype is a recent example showing how criminals can use it to attack people's privacy. Namely, severe vulnerability is found in Skype that makes it possible to steal the user's account by using only the email address associated with it. It is only necessary to register a new Skype account and enter the victim's email address. Then a third party log in with its new user's account requiring password reset providing the victim's account /**1**/. The client who logs in with a new account is given the Skype password reset token, then he changes the password and gets the access to the victim's account. The only way to protect from such at-

tacks is to have a secret email address associated with the Skype account. Another example of disturbing privacy on daily basis occurs while surfing the Internet. According to the recent research done by development team of the Ghostery company, some firms use over 100 various trackers of the Internet users. 137 of them have been found on the Microsoft and 106 on the Apple web pages. The companies use them to collect information about users on the open browser pages or by tracking the number of visits to certain pages, etc /**2**/. Other examples illustrate vulnerability of Microsoft's Hotmail and Outlook accounts which lies in the authentication procedure of Hotmail and Outlook email services for Microsoft to validate user's login information making it much easier for the attackers to steal users' accounts. User credentials are validated by authentication cookie of the web browser and still remain successful although the victim logged out before the cookie 'theft'. Entering the stolen cookies into a person's web browser is not technically demanding, nor is their stealing if the victim's computer is accessible. However, there are manners how to steal them without having the access to the computer or its network, the best known among them is cross site scripting (XSS) /**3**/. Also, one interesting way of identity theft is via memory stick. Identity can be stolen in this way within maximum of 30 seconds. How? When the memory stick is inserted into the computer then something that most people regard as 'terribly good' thing about Windows XP is run, the so-called auto play. While Auto play is running, if the memory stick is infected by some malicious software, its software code spreads on your computer and after that a creator of the malicious software takes control over it. To protect against such type of malware attack you should disable the Windows Auto play option (40% job is done after turning off Auto play option). Also, it is suggested not to insert unsafe memory sticks into computer, namely, format sticks when you find them, of course, if you want to use them, but never view their contents without previous checking and using protection! It is important to know that a good money can be made by selling identity today, from 50 Eurocents to $20 per identity, add to this connecting computers to the botnet which enormously multiplies the amount and profit of the identity thieves. Numerous examples worldwide show the amounts of the damages inflicted but we will mention only some of them: Example 1 3.6 million of social security numbers were stolen from Americans /**4**/.

In South Carolina 3.6 million of social security numbers were stolen. Identification numbers are frequently used in identity theft as it is assumed that only their users know them. Also, 387.000 credit/debit card numbers were stolen from the attacked server. Example 2 47 million dollars stolen from 30,000 bank accounts /**5**/. Zeus, a variation of Troyan horse malicious software was to blame for recent theft of $47 million from over 30.000 bank accounts. In the attack was used Zeus Troyan for mobile platforms ZITMO (aka Zeus in the mobile) designed to pass the user's two-level-authentication by sending SMS. After infecting the user's computer, in the first attempt to access a bank account, the online banking 'upgraded' virus infected version for mobile devices was sent to the victim. The virus enabled the access and carrying out money transactions from the victim's bank account.

Example 3 The US police discovered massive money theft in credit card fraud /**6**/. Gang of 18 people was charged with stealing $200 million in credit card fraud as has been found so far. They invented more than 7 thousand false identities, opened more than 25 thousand credit/debit card accounts in Pakistan, Canada, India, the UK and elsewhere. They never meant to cover overdraft on bank accounts they made and only after a year and half long investigation the police found $70.000 hidden by a thief in his oven. They spent the money on buying gold, luxurious cars, electronic gadgets and on spa treatments.

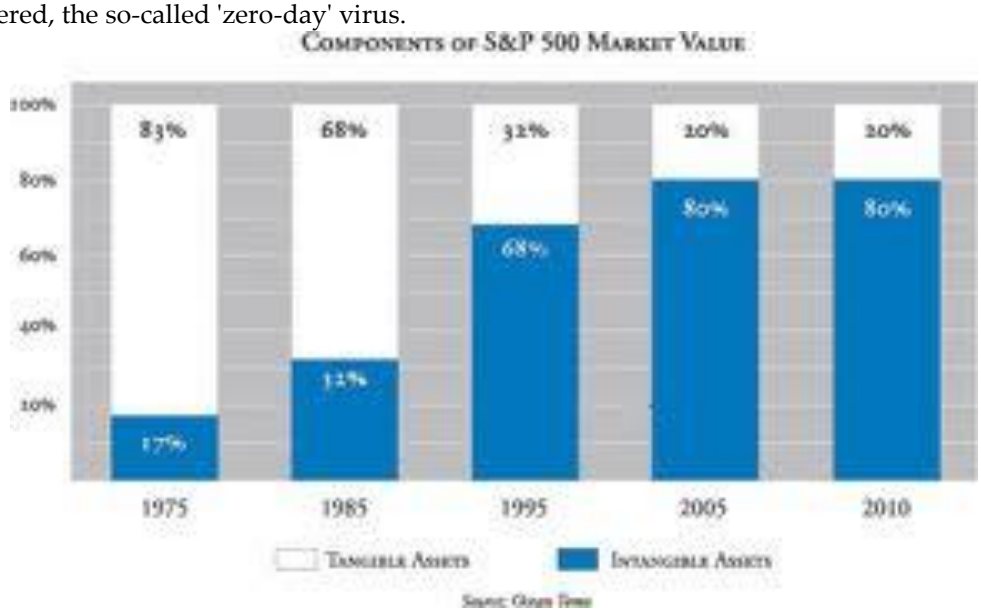
Example 4 658 million $ lost in phishing /**7**/.

RSA security group released their survey results claiming that the number of computer security incidents increased for 10% in the first half of the year 2012 compared with the same period in the previous year. They referred to phishing as the biggest threat due to the attackers' convincing tactics and users' unthoughtfulness. Social networks such as Face book are most frequently mentioned as the

starting point of attack due to the amount of private information that users' accounts provide. Example 5 99% attacks is enabled by non-regular use of patch applications/**8**/.
Microsoft's experts warn that over 99% attacks are enabled by failures in users' applications. Users might regularly install patches for their operating system yet, they do not regularly install the patches for other programs they use. This is the main way in which the attackers take control over users' computers or steal the users' data. Less than 1% of attacks use till then undiscovered, the so-called 'zero-day' virus.

2 Intellectual capital and identity fraud

Intellectual capital theory is a prominent new theory which largely promise improvement in future business outcomes. The fact is that tangible assets (land, buildings, equipment and money) of the world leading companies today have less value than intangible assets which are not mentioned in their business balances /**9**/.



According to this theory, a company's value is based on human capital, structural capital and customer capital. Building value means converting one form of capital into another. For example, new value is made when human ability (human capital) creates new business processes (structural capital) resulting in improved services for consumers, increasing their loyalty (consumer capital). One of the main features of intellectual capital is its intangibility. *Intellectual capital is intangible asset. Intellectual capital is also described as 'hidden asset'. Therefore it is often hard to identify and estimate its market value.* Tacit (hidden) knowledge is the most important source of a company's competitive advantage because it is 'stored' into the heads of individuals including the following features: great value, scarcity and impossibility to imitate. Each company should try to convert this hidden – tacit knowledge into explicit, codified, i.e. materialized knowledge that becomes the knowledge owned by a company transformed into structural capital /**10**/. Back in 2004, the US president asked NIAC to find out how the USA could provide safe proper development of intellectual capital to protect US critical information infrastructure and infrastructural concept /**11**/. It should be pointed out that investment in intellectual capital is the value that pays off many-fold which is the fact recognized by the UK whose investments in intellectual capital sector in the period between 2011-2012, within which 16 projects, were supported by more than 1,600 000 000 kn /**12**/. Some of sub-sets of intellectual capital include human capital, information capital, brand awareness and instructional capital. But its structure, according to most today's theoreticians includes the following: human capital, structural (or organizational) capital and relational (or consumer) capital /**13**/. Intellectual capital is the value of a company or organiza-

tion's employee knowledge, business training and any proprietary information that can provide the company with a competitive advantage. Intellectual capital is considered an asset, and in a broader sense can be defined as the collection of all informational resources a company has at its disposal that can be used to drive profits, gain new customers, create new products, or otherwise improve the business.
Intellectual capital itself, according to some authors, is a complex economic category representing all business factors which are not explicit in traditional business analysis, yet, they make additional value in an organization considerably influencing long-term profitability and competitiveness of a company. Intellectual property is an important component of company's intellectual capital, it is entirely materialized, codified knowledge: patents, licences, copyrights, franchises, software, and all other materialized value of human capital ICT is as a part of intellectual capital the use of which increases synergy between employees and clients of a company. ICT converts intellectual capital into a particular competitive advantage of each company that recognizes its own intellectual capital as a resource /**14**/. Finally, knowledge and intellectual capital as intangible assets are becoming a basis of competitive advantage of an enterprise. Referring to the last two above mentioned components of intellectual capital, i.e. intellectual asset, it is not hard to conclude that they are recognized and highly ranked as the attack targets of identity theft since the profit is multifold higher compared with the profit of other targets attacked by the same method. Considering the above mentioned, the risk analysis should include a high probability degree in the identity fraud threat and dedicates a particular segment of security policy to the methods and techniques of fighting against such forms of threats.

3 International and Croatia's legal framework

Referring to the international legal framework we could say that the Convention on Cybercrime and the Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems make a good legal grounds to harmonise substantive law provisions which enable efficient fighting against illegal acts such as identity fraud. It should be pointed out that the Convention on Cybercrime adopted in Budapest on November 23, 2001, released in "Narodne novine" – Međunarodni ugovori« br. 9/2002, came into force in the Republic of Croatia on July 1, 2004, while Additional Protocol concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems drawn up in Strasbourg on January 28, 2003, released in " Narodne novine" – Međunarodni ugovori« br. 4/2008, came into force in the Republic of Croatia on November 1, 2008 /**15**/. According to the new Penal Code of the Republic of Croatia which came into force on January 1, 2013, identity theft is not explicitly defined as criminal offence. It does not necessarily mean that in the Republic of Croatia identity fraud as a criminal offence is not given due attention since it is done under the existing legal provisions which in some aspects provide broader protection or as good as the one included in the Convention. An example - in accordance with legal provision, Article 266, Prov.1 Chapter 25 (criminal offences against computer systems, programs and data).
In accordance with Penal Code, Article 266.
Unauthorized access:
(1) Whoever, without authorization accesses the computer systems or data of another shall be punished by imprisonment not exceeding one year," illegal (unauthorized) access to the computer systems, data or programs is punished by imprisonment not exceeding one year. It is obvious that regardless of motif or goal, unauthorized access is criminalized. With regard to criminal offence committed intentionally, only dolus act is needed (intentional unauthorized access). If the criminal offence referred to in paragraph 2, of the same Article is perpetrated (qualified form):
(2) If the criminal offence referred to in paragraph 1, of the same Article is committed in connection with the computer system or electronic data of a governmental body, local or regional self-governmental bodies a public institution or a company of special public interest, the perpetrator shall be punished by imprisonment not exceeding three years. However, if the damage is caused to property

while the perpetrator acts, the perpetrator can be criminalized for concurrence of offences in accordance with Article 235 of the Penal Code: Inflicting damage to another person's property Article 235.

(1) Whoever damages, deforms, destroys or renders unusable another person's property shall be punished by imprisonment not exceeding two years.

(2) The punishment referred to in paragraph 1 of this Article shall be inflicted on a perpetrator for unauthorized embellishment of walls, motor vehicles or other public surfaces Larceny, Article 228 of the Penal Code(3) If the criminal offence referred to in paragraph 1 or 2 of this Article is committed from base motives or caused significant damage, a perpetrator shall be punished by imprisonment for six months to five years.

(1) Whoever takes away the movable property of another with an aim to unlawfully appropriate it shall be punished by imprisonment for six months to five years.

(2) If the stolen property is of small value and the perpetrator acts with an aim to appropriate the property of such value, he shall be punished by imprisonment not exceeding one year.

(3) If the perpetrator returns the stolen property to the injured party prior to learning that he has been discovered, the court may remit the punishment.

For example, in case of the stolen media itself (hardware), certain devices such as modems or other media where data are stored or in case of destroyed or damaged media. Along with the criminal offence from the Article 266, paragraph 1 of Penal Code, the identity theft can be recognized in another criminal offence such as unauthorized access to personal data with the aim of fabricating a false document or false credit cards or selling false credit cards via the Internet as well as using other person's card personal data to charge the owner's bank account for buying goods or withdrawing the money. Concurrence of offences is possible with another criminal offence as referred to in the Article 266 of the Penal Code. Furthermore, by provision of the Article 267, paragraph 1, of the Penal Code Computer system interference, Article 267, of the Penal Code:

(1) "Whoever renders unusable or hinders the work or the use of computer systems, electronic data or computer programs or communication , " criminalization is directed to rendering unusable or inaccessible other person's computer data or programs or computer communications.

Criminal offence perpetrated:

Damage to computer data, Article 268.

(1)" Whoever without authorization damages, alters, deletes, destroys or in some other way renders unusable or inaccessible the electronic data or computer programs," includes unauthorized damages and perpetration of all other specified criminal offences rendering the electronic data inaccessible (which refers to the Article 4 of the Convention).

Description of the criminal offence is more extensive than in the Convention:

„Unauthorized interception of computer data," Article 269.

(1) „Whoever intercepts or records the non-public transmission of electronic data to, within or from a computer system, not intended for his use, including the electromagnetic transmissions of data in the computer system, or enables an unauthorized person to access these data," as apart from interception it extends to unlawful computer program manipulation.

The purpose of criminalization in the Article 269 of the Penal Code is protection of non-public, private communication as referred to in the Article 3 of the Convention. This provision gives broader protection since it includes third party (a person) who gets access to electronic data. A third party is every person who is not authorized to have access to electronic data including electromagnetic transmission of data into the computer system.

To perpetrate the offence it is enough to enable data access to a third party regardless whether or not the person is really familiar with the data. A person who was authorized to record electronic data (e.g. security service and others) shall be punished for this criminal offence if the record was passed to a third party. The criminal offence includes all computer data regardless of the way of their transmission (email, telephone, fax, etc.). There is a possibility of a concurrence of offences with criminal offences such as disclosure of personal and

family conditions: "Unauthorized use of personal data," Article 146.
(2) Whoever, contrary to the provision referred to in the Code, passes personal data from the Republic of Croatia for the purpose of further processing or releasing or making them accessible to a third party in any other way, or by undertaking actions as referred to in the Item 1 of this Article, procures unlawful pecuniary gain for himself or a third party or causes significant damage,
"Extortion," Article 243.
(1) Whoever, with an aim to procure unlawful pecuniary gain for himself or a third party, by force or by a serious threat induces another person to do or to omit to do something to the detriment of his property or the property of another, or by unauthorized technical recording or eavesdropping.
„Unauthorized technical recording or eavesdropping," Article 143.
(1) Whoever, without authorization audio records non-public spoken words of another person or eavesdrops non-public spoken words of another person not addressed to him."
"Unauthorized image recording," Article 144.
(1) Whoever, without authorization, records the image of another person in his flat or a space specially protected from views or uses the image or makes it accessible to a third party violating the privacy etc.
Furthermore, Article 273. of the Penal Code:
"Serious criminal offences against computer systems, programs and data." Article 273
(1) If the criminal offense referred to from the Article 267 to the Article 270 of the Penal Code is committed in connection with the computer system or electronic data or computer program of a governmental body, or regional self-governmental body, a public institution or a company of special public interest," provides more extensive protection since the criminal offences referred to from the Article 267 to the Article 270 if significant damage is caused, but also with regard to special importance of data for the public government, institution or a company of special public interest. It should be emphasized that in accordance with legal concept of the Supreme Court Criminal Department of the Republic of Croatia, significant damage exceeds the value of 30.000 kn.

The purpose of the provision of the Article 272 of the Penal Code:
„Misuse of devices," Article 272.
(1) Whoever produces, procures, sells, possesses or makes available to another person special devices, computer programs and electronic data created or adapted for the perpetration of the criminal offence referred to in the Article 266, the Article 267 and the Article 268, the Article 269, the Article 270 and the Article 271 of this Code, with an aim to use them for perpetrating some of these offences," is to prevent making and spreading a „black market" of the devices and means which are suitable for perpetration of criminal offences as referred to in the Article 266 to the Article 271 of the Penal Code. Although the provision refers to the Article 6 provision of the Convention it provides more extensive protection. Namely, it deals with punishment of intentional unauthorized act:
(2) Whoever produces, procures, sells, possesses or makes accessible the computer passwords or other data to access the computer system with the aim of perpetrating criminal offences referred to in the Article 266, the Article 267, the Article 268, the Article 269, the Article 270, the Article 271 of the Penal Code, "
The goal of the above mentioned paragraph is also important.
In accordance with the provision of the paragraph 4 of this Article further procedure with such devices and procured data is stipulated as follows:
(4) Special devices, programs referred to in the paragraph 1 of this Article shall be forfeited and the data referred to in the paragraphs 1 and 2 of this Article, shall be destroyed."
In accordance with provision of the paragraph 4 of the Article 270 of the Penal Code which refers to provisions of the Article 7 of the Convention:
Computer-related forgery, Article 270:
(1) Whoever, without authorization, develops, installs, alters, deletes or makes unusable computer data or programs that are of significance for legal relations
in order for them to be used as authentic, or whoever uses such data or procures them to be used"', also provides more extensive protection than the Convention, Namely, protection

is more extensive as the criminal offence as referred to in the Article 273 is defined as perpetration of criminal offence from the paragraph 1 of this Article if significant damage is inflicted in connation with electronic data or programs of governmental bodies, public institutions or companies of particular public interest .

Article 272 ensures legal penalty in an early stage, prior to perpetration of another criminal offence. In this case as well, and in accordance with the provision of the paragraph 4, Article 272. devices are forfeited and due to the significance of protected values and gravity of offence as referred to in the paragraph 5, whoever attempts to perpetrate the criminal offences as referred to in the paragraph 1, shall be punished.

Provisions of the Article 271 of the Penal Code refer to the provision of the Article 8 of the Convention which stipulates Computer fraud:

(1) Whoever, with an aim to procure unlawful pecuniary gain for himself or a third party, alters, develops, deletes, damages or in some other way renders unusable or inaccessible the electronic data or computer programs of another," also ensures more extensive protection that the Convention. Namely, in accordance with the provision of the paragraph 1, whoever perpetrates criminal offence of computer fraud will be inflicted particular punishment if the criminal offence is perpetrated with the only aim to inflict damage to another. So, special punishment is included for intentional inflicting the damage to another as the only aim. Regardless whether or not unlawful pecuniary gain is procured. In this case, in accordance with provision in the Article 272, devices are forfeited.

Regarding offences related to infringements of copyright and related rights, although the Convention gives options to choose protection through civil and legislative institutions, Croatia enables criminal-law protection apart from civil and legal protection of copyright and related rights in the following cases:

Chapter 27: Criminal offences against intellectual property, Violation of personal rights of an author or a performing artist, Article 284: Unauthorized use of work of authorship or a performance of a performing artist, Article 285: Infringement of other copyright and related rights, Article 286.

From the all afore mentioned, it is obvious that the identity theft in the Republic of Croatia as a criminal offence can be successfully fought against within the existing legal framework.

4 Conclusion

Identity theft in its various forms is currently becoming frequent criminal offence relying above all on ICT, since ICT, despite its many good sides, has brought its users certain weaknesses i.e. vulnerabilities. Risk analysis of the ICT-aided systems is a necessary prerequisite for building security policy which must recognize the identity theft and fraud as objective and highly ranked threats. Intellectual capital must be particularly recognized as the future big target of identity theft apart from all so far known, as it hides great values in itself and I would specially point out the intellectual property being of particular interest to identity thieves. Current legal framework in the Republic of Croatia provides a prerequisite for efficient fight against identity theft, although it is not explicitly recognized as a criminal offence which is the case in some EU and the world states. Therefore, further possibilities of national legislation development should be reconsidered in an attempt to find better solutions, especially in the procedural domain that would strengthen the state machinery in fighting against identity theft and fraud.

Notes

/1/ Matija, Mandarić, Kritičan propust u Skypeu dovodi u pitanje vašu privatnost, (14.11.2012.), URL: https://sigurnost.carnet.hr/svijet-o-sigurnosti/novosti/ranjivost-u-skypeu/. (26.04.2013.).

/2/ Zoran, Vlah. Facebook prikuplja brojeve telefona, (01.07.2013.), URL:https://security.carnet.hr/svijet-o-sigurnosti/novosti/tag/privatnos. (16.04.2013.).

/3/ Matija, Mandarić, Ranjivost u Microsoft Hotmail i Outlook računima, (17.12.2012.), https://sigurnost.carnet.hr/svijet-o-sigurnosti/novosti/ranjivost-u-microsoft-hotmail-i-outlook-racunima/. (14.04.2013.).

/4/ Matija, Mandarić, Amerikancima ukradeno 3,6 milijuna identifikacijskih brojeva, (29.10.2012.),

URL:https://sigurnost.carnet.hr/svijet-o-sigurnosti/novosti/ukradeno-3-6-milijuna-identifikacijskih-brojeva-americkih-gradjana/. (15.04.2013.).

/5/ Matija, Mandarić, Ukradeno 47 milijuna dolara s 30 tisuća bankovnih računa, (06.12.2012.), https://sigurnost.carnet.hr/svijet-o-sigurnosti/novosti/ukradeno-47-milijuna-dolara-s-30-tisuca-bankovnih-racuna/. (25.04.2013.).

/6/ Američka policija otkrila veliku prijevaru težku više od 200 milijuna dolara, (06.02.2013.), URL:http://www.poslovnipuls.com/2013/02/06/americka-policija-otkrila-veliku-prijevaru-tesku-vise-od-200-milijuna-dolara/. (21.04.2013.).

/7/ Matija, Mandarić, Phishing zaslužan za gubitke od 658 milijuna dolara, (24.08.2012.), URL:https://sigurnost.carnet.hr/svijet-o-sigurnosti/novosti/phishing-zasluzan-za-gubitke-preko-658-milijona-dolara/. (21.04.2013.).

/8/ Matija, Mandarić, 99% napada omogućeno ne redovitim zakrpama, (28.06.2012.), https://sigurnost.carnet.hr/svijet-o-sigurnosti/novosti/99-napada-omoguceno-ne-redovitim-zakrpama/. (20.04.2013.).

/9/ Convention on Cybercrime, (2002.), URL: http://narodne-novi-ne.nn.hr/clanci/medunarodni/2002_07_9_119.html.(10.04.2013.).

/10/ Penal Code, (2011.), URL:http://narodne-novi-ne.nn.hr/clanci/sluzbeni/2011_11_125_2498.html.(10.04.2013.).

/11/ Gary R. Comstock, The Growing Need for Secure Enterprise Search, (2011.), URL:http://www.edatafusion.com/whitepaper. (02.04.2013.).

/12/ *Marko, Kolaković, Teorija intelektualnog kapitala, (2013.)*, URL:http://hrcak.srce.hr/file/40500. (21.04.2013.).

/13/ Dragomir, Sundač, Švast, Nataša, Intelektualni capital, temeljni čimbenik učinkovitosti poduzeća, (2009.), URL:http://eobrazovanje.mingorp.hr/UserDocsImages/Knjizica_intelektualni_kapital.pdf. (02.04.2013.).

/14/ Europe 2020: UK National Reform Programme 2013, (April, 2013), URL:http://ec.europa.eu/europe2020/pdf/nd/nrp2013_uk_en.pdf. (07.04.2013.).

/15/ George, W. Bush, National Infrastructure Advisory Council, (11. 06. 2006.), URL:http://www.dhs.gov/xlibrary/assets/niac/niac_workforcereport_transltr.pdf. (05.04.2013.).