UDK 004.056.5
Preliminary communication

# INFORMATION SYSTEM SECURITY THREATS CLASSIFICATIONS

**Sandro Gerić, Željko Hutinski**
University of Zagreb, Faculty of organization and informatics, Varaždin, Croatia
*{sandro.geric, zeljko.hutinski}@foi.hr*

**Abstract:** *Information systems are exposed to different types of security risks. The consequences of information systems security (ISS) breaches can vary from e.g. damaging the data base integrity to physical "destruction" of entire information system facilities, and can result with minor disruptions in less important segments of information systems, or with significant interruptions in information systems functionality. The sources of security risks are different, and can origin from inside or outside of information system facility, and can be intentional or unintentional. The precise calculation of loses caused by such incidents is often not possible because a number of small scale ISS incidents are never detected, or detected with a significant time delay, a part of incidents are interpreted as an accidental mistakes, and all that results with an underestimation of ISS risks. This paper addresses the different types and criteria of information system security risks (threats) classification and gives an overview of most common classifications used in literature and in practice. We define a common set of criteria that can be used for information system security threats classification, which will enable the comparison and evaluation of different security threats from different security threats classifications.*

**Keywords:** *information system security, ISS, security risk, threat, classification, criteria.*

## 1. INTRODUCTION

Information systems (IS) are exposed to different types of security threats which can result with significant financial loses and damage to the information system resources. The types of damage caused by security threats are different, e.g. database integrity security breaches, physical destruction of entire information systems facility caused by fire, flood, etc. The source of those threats can be unwanted activities of "reliable" employees, hacker's attacks, accidental mistakes in data entry, etc. The financial losses caused by security breaches often can not be exactly defined because of the facts that significant numbers of smaller scale security incidents are never discovered, a part of incidents are described as accidental mistakes, and all of that is a result of a tendency to minimize the responsibility of a person responsible for the security incident [2.][4.][5.].

Security threat can be defined as every event that can result with information confidentiality, integrity and availability breaches, or with any other form of information system resources damage. The security threats consequences are different, so some security threats have influence on confidentiality or reliability of stored data, and some threats have influence on functionality and efficiency of entire information system. Security threats can

be observed and classified on different ways and different criteria. A motivation for this article arises from the information system security survey conducted by authors in 2005. and 2006.. This survey has shown that the level of information system security in Croatian companies is relatively low. There are significant differences in security level by different economic sectors, e.g. financial and ICT versus manufacturing and sales & retail sector. The total number of business organizations that participated in survey was 60 (36 participants in the 2005. and 24 participants in 2006.). The Croatian companies that participated in survey were grouped in following groups based on their common characteristics: manufacturing, sales and retail, ICT sector, financial sector (banks, financial funds, insurances), and public administration. For this paper two survey questions are interested – questions regarding the information system security threat classifications. Precisely,

1. *Does your organization systematically monitor and record the information system security threats to which it is exposed?* and
2. *Does your organization use any of described information system security threat classifications for ISS threats monitoring?*

Only 10,81% of survey participants in 2005. conducted systematical monitoring and recording of information system security threats to which their organization is exposed to. The majority of organizations that have answered *yes* on this question comes from ICT sector (21,43%) and financial sector (11,11%).
Only 8,82% of participant used one of internationally defined and recognized information system security threat classifications. The best situation was in ICT sector where 14,28% has systematical record and use information system security threats classification and financial sector (11,11%). The two ISS threat classifications (ISO/IEC 17799) and simplified NIST classification were mostly used.
These results motivated us to describe the most important security threats (ISS) classifications, and to develop gives a new hybrid model which can be implemented in every environment as a template for ISS threat monitoring and classifying.

## 2. SECURITY THREATS CLASSIFICATIONS – AN OVERVIEW

In the domain of information system security different types of security threats classifications are used. The reason why threats classifications are necessary comes from the fact that if information systems resources should be protected we have to know the sources and the threats from which we are protecting it [6.][7.]. The problem exists at the point when we have to compare two or more security threat classifications that are incompatible. At that point the usual solution is to combine compared classifications and create a hybrid and temporary one that will usually be used only for a short period of time. An authors of security threat classification are various – from international, governmental and nongovernmental institutions, scientists, practitioners, ISS experts, etc. In this section we give an overview of most usually used information security threats classifications.
*NIST classification* [14.] is based on ISS threats significance criteria, and distinguished following types of security threats:

1. *Errors and omissions* – are significant security threats that are usually underestimated. But, if we define security threats as every event that can lead to information systems (hardware, software, data ware, life ware) integrity breaches, then errors and omissions are security threats. The most common cause for errors and omissions are intentional human mistakes. This type of security threat can be caused by employees that are entering a hundreds of database entries on daily bases, but also by users that are

responsible for data sources. The problem with errors and omissions is the fact that it is not possible to build-in application's mechanisms for every possible types of (data entry) errors control. The solution is to improve the working conditions and employee's education, and employees' awareness for this type of security threats. This type of security threat is not limited only on data entry processes, but it can happen during the programming and information systems development processes (e.g. accidental mistakes in manual programming), user's right definitions, what all can result with significant and serious consequences on information system security. The information system security threats survey conducted by R. Couortney showed that almost 65% of all information system security threats are errors and omissions, whether accidental or deliberate nature [14.]. The especially dangerous type of errors and omissions are those that are occurring during the programming processes, and they are usually referred to as "bugs". Bugs can be everything from harmless mistakes to mistakes that will result with application malfunctions, what will at the end result with high expenses necessary for later debugging processes. Beside financial loses those types of mistakes have significant influence on company profile and image [14.].

2. *Fraud and theft* – are form of security a threat than can be performed by simply automating "traditional" forms of fraud and theft, or can be performed using more modern methods. For example, employer can use the computer (and program) for steeling small amounts of money from financial accounts with presumption that the small financial transaction will not be checked as suspicious (and a large number of small financial amounts can result with significant total amount of stolen money). But, the object of this type security threats are not just financial systems, but every other system that have any type of access control role to different resources (e.g. warehouse information system, public institutions information system, telecommunication information system). The computer frauds and thefts can be performed by *insiders* and *outsiders* [9.]. Insiders are persons, employees that are authorized system users who are using the system on daily bases for every day work assignments. It is interested that the majority of these threats origin from insiders. There are several explanations for this: they have (unlimited) accesses to information systems resources, are well familiar with system resources and security controls, and know the possibilities for fraud (and theft) and the potential value of these actions. Based on those facts U.S. Department of Justice's Computer Crime Unit contends that "insiders constitute the greatest threat to computer systems" [14.]. Besides the possibility that information system resources can be used for committing fraud or theft, they can be a subject of a theft themselves. Safeware insurance analysis showed that the $882 million worth of personal computers was lost due to the theft in 2002. [14.]

3. *Employee sabotage* – is often security threats to which are exposed information systems resources. As already mentioned insiders are persons that are the best familiar with system resources, performances and capabilities, so they are also familiar with information system areas where they can cause the most damage. If this is connected with unsatisfied employees there exists a real danger of sabotage actions from existing or former employee. Although the proportion of employee sabotage in total information system security threats is lower then the portion of fraud and theft, the consequences of this threat can be substantial. The most often examples of sabotage are [14.]:

    a. Destroying hardware of facilities,

    b. Planting logic bombs that destroy programs or data,

c. Entering data incorrectly,

d. "crashing" systems,

e. Deleting data,

f. Holding data hostage,

g. Changing data.

4. *Loss of Physical and Infrastructure Support* – can be realized on many different ways, e.g. loss of electricity supply, loss of communications, flood, fire, earthquake, strikes, etc. It is type of information system security threat that can not be under full control of information system's resources owners, and that can potentially have a significant influence on information system functionality [14.].

5. *Hackers* – are relatively new threat to information system security that is becoming more and more important with Internet and communications network development. The term *hacker* refers to person that on an unauthorized way tries to approach and (mis)use the information system resources. Although the scope of damages caused by hackers is far less significant then damages caused by fraud or theft, their influence can be larger [13.]. The fact that hackers are often steeling data (e.g. credit card numbers) makes them a new – hybrid type of threat. However it is positive that hacker's activities are becoming more and more attention, not only from newspapers, but also from information system security experts. According to U.S. Department of Justice's Computer Crime Unit there are three basic reasons for this [14.]:

   *a.* The sources of this threat are usually outsiders, and because of that the organization does not have appropriate mechanisms necessary for sanctioning these activities.

   *b.* The main goal of hackers attack is often unknown. It could be data theft, deletion or unauthorized changing of data, or simply hacker wants to point out systems flows and bugs.

   *c.* Hacker's attack makes people vulnerable – they attack with out special reason, and it is not possible to anticipate the kind of damage they will produce.

6. *Malware* – is a type of security threat that encompass different types of computer viruses, Trojan horses, worms, logical bombs, and other form of "unwanted" software. The most significant threats of this kind are [14.]:

   *a.* *Computer viruses* – parts of program code that are individually replicated and attached with executable files. When user starts an exe file it automatically starts the attached virus. Computer viruses can perform different activities on user's computer – from harmless (e.g. writing messages on screen) to more serious (e.g. disk formatting).

   *b.* *Trojan horses* – are programs that are installing them selves automatically on user's computer and are performing different, unwanted, activities.

   *c.* *Worms* – programs that are by automatically execution extremely decreasing systems performances.

7. *Threats to personal privacy* – are emerging type of security threats. Large amounts of personal data that are stored in different databases (e.g. public and private institutions,

banks, companies) can . There is a real threat that those kinds of personal data could be misused in many different ways (the "Big Brother" conspiracy theory) [14.].

*CSI/FBI Computer Crime and Security Survey 2004* [8.] classification as criteria uses the ISS threat source. According to CSI/FBI classification there are two main types of information system security threats, based on the position of security threat source based on attacked information system. The source of threat can be inside or outside the attacked system. The organizations and their security systems are usually focused on protecting them selves from threats that are origin from outside the system. The threats that are coming from inside are often not considered. The *CSI/FBI Computer Crime and Security Survey 2004* [8.] have shown that the majority of security incidents is provoked from organization's inside, and those threats are usually mistakes (almost 39% [8.] of all internal security threats are employee mistakes). The most significant threats that are origin from outside of organization system are different types of *malware* (computer viruses, Trojan horses) *spam*, *phising* and *denial of service attacks*. Spam (or unwanted e-mails) becomes more significant problem because it blocks network traffic and can be used as a transport tool for *malware* software, frauds, etc. Almost two thirds of all e-mail messages exchanged during the September of 2004. were spam messages [16.]. One of the latest forms of computer fraud is *phising*. It is a type of security threat that can be conducted on several ways, and most often the victim receive a forged e-mail message that is very similar to the official correspondence from bank or financial institutions [17.]. In *phishing* message the sender explains that for some reasons the victim should enter and send their personal data (including their bank account number, PIN, etc) in an attached web form. The message and the form does not represent the official correspondences and are used for stealing personal data (including the bank account numbers), and the victim became a victim of "identity theft" [13.]. Increase dependency on communication networks resulted with a new form of security threat – *Denial of Service*, or *DoS* attacks. The idea behind a *DoS* attacks is to block the companies system (e.g. communication system, web shop) with a large number of sent messages, requests, etc. This type of attack can be especially dangerous if is directed on a company that is based on e-commerce or that depends on communication services [12.][15.]. Besides the individual companies, DoS attacks are often directed on large telecommunications area what can result with significant decrease in functionality of telecommunication services.

The third classification presented in this paper was defined by *Sieber* [3.]. Sieber distinguishes security threats based on their consequences. The results of these criteria are the following types of security threats [3.]:

1. *Privacy intrusions* – identical to "*Threats to personal privacy"* from NIST classification,
2. *Computer economic crime* - in form of computer manipulation, computer sabotage, computer extortion, hacking, computer espionage, software piracy),
3. *Threats to communications,* and
4. *Other information system security threats*.

Another theoretical, and not so detailed information system security threat classification, is the one by *Wasik* [3.]. He distinguished three main groups of information system security threats [3.]:

1. *Unauthorized access and use,*
2. *Fraud and information theft,* and
3. *Similar threats.*

Based on *OECD* report on information systems security another proposal for information system security threat classification was made. It consists of five groups of security threats that should be considered by information system security development. Those groups are [3.]:

1. deliberate entering, changing, deleting and/or un-ableling the use of computer data and/or computer programs with intentions to perform an *illegal fund or values transfer*,
2. deliberate entering, changing, deleting and/or un-ableling the use of computer data and/or computer programs with intentions to perform *forgery*,
3. deliberate entering, changing, deleting and/or un-ableling the use of computer data and/or computer programs, or other disturbances in information system with intentions to *disable the normal functioning* of system,
4. the *breaches of exclusive copy and owner rights* on protected computer source code,
5. deliberate *access or un-ableling the access* to computer and/or telecommunication system, performed *without necessary authentication* by security measures breach or on any other unfair attentions.

This proposal finally evolved in a *Recommendation (89)9* of European Council. This recommendation defines a minimal and additional list for acts in the computer crime domain that should be sanctioned by member countries. The list consists of following main security threats [3.]:

1. computer frauds,
2. computer forgery,
3. damaging of computer data or programs,
4. computer sabotage and unauthorized access,
5. unauthorized ear tapping,
6. unauthorized reproduction of protected computer programs,
7. unauthorized copying of semiconductor elements topography,

and additional security threats:

8. unauthorized change in computer data and/or programs,
9. computer espionage,
10. unauthorized use of computer system, and
11. unauthorized copying of protected computer programs.

A security threat classification that emerged from international *ISO/IEC 17799:2000* standard distinguishes security threats by the type of their sources [18.]. Based on that criterion four main groups of security threats can be defined [10.][11.]:

1. source – *nature*: earthquake, flood, storm, pollution, fire, incidents;
2. source – *technical*: technical mistakes, malfunctions, communications errors, radiation,
3. source – *people with attribution of un-attentiality*: indiscipline, negligence, inappropriate software, inappropriate organization.
4. source – people with attribution of attentiality: destruction, sabotage, diversion, espionage, war destruction, fraud, steeling, viruses.

Some authors [1.] are using the activity area on which security threat is focused as a main criterion for information system security threat classification. According to this four main group, with several subgroups, of security threats can be defined. The groups are:

1. *intrusion on physical security* [1.]:
    a. *Ear tapping of wired communications* – a security threat that uses the insufficient (and often nonexistent) protection of physical communication channels (e.g. wires, communication cables) with purpose to eartapp the communications pathways (and in combination with this illegal data access) [1.].
    b. *Denial of Service* – as already mentioned before this security threat is focused on limiting the functionality and availability of information system resources. Availability of information system resources, in the context of information system security, assumes that all capabilities of information system resources, like information system infrastructure, software, etc. will be available for authorized user. Degradation of IS services can be caused on many different ways [17.] – physical assault, backup systems malfunction, natural disasters – what all can result with a physical damage to the information system, etc. [1.]
    c. *Trash digging* – security threat that is not illegal because it is based on searching through garbage – unwanted and discarded resources. It is interesting that this type of security threat can lead to serious damage, because in garbage different resources, like un-erased data media, non-shredded paper documents, etc., and indirectly many information valuable for organization, can be found [1.].
2. *intrusion on personnel security* [1.]*:*
    a. *User's password guessing* – the intruder tries to and guess the user's password, and then to use this password for unauthorized activities. This attack can be conducted manually and automatically. This way in relatively short period of time large number of possible password candidates can be checked.
    b. *Masquerading* – also known as "false identity" is a type of security threat where one person uses the identity of another person with purpose to gain access to information system infrastructure. Masquerading can be physical (use of authorized user's identity and/or user's identity card), and electronically (use of electronic user's identity with purpose to log in the information system).

c. *Social engineering* – different ways of manipulations with purpose to gain access to useful information (user names, passwords, business secrets, etc.) that can be used to endanger the information system security [1.].

d. *Extortions* – different types of extortions from persons that have access to (classified) information necessary for information system security breach.

e. *Software piracy* – illegal copying and use of software.

3. *intrusion on communication and data security* [1.]:

   a. *Attacks on data* – threats that are focused on data confidentiality, availability and integrity.

   b. *Attacks on software* – different types of *malware* software that was described in the previous sections (e.g. computer viruses, worms, Trojan horses, back doors, timed attacks, hoaxes).

4. *intrusion on operational security* [1.]:

   a. *Data frauds* – also known as false data entry is basically unauthorized change of data entry prior, during or after the data store in information system.

   b. *Spoofing* – a type of security threat in which attackers will gain wanted data by using weaknesses of Internet and insufficient attention of the users.

   c. *Sniffing* – threat that use malicious software with purpose to sniff – to exam the network traffic in search for part in which user names and passwords are exchanged [1.].

   d. *Searching* - threat that use malicious software with purpose to search the network systems for information that are used for unauthorized activities.

   e. *Privileged access* – threat that rise from the administrator and privileged user rights and their misuse.

## 3. THE NEW MODEL OF INFORMATION SYSTEM SECURITY THREAT CLASSIFICATION

Existing models and information system security threat classifications are usually limited on use of one or two criteria as a base for security threat classification. This is sufficient for stable environment where security threats are relatively stable, but in the constantly changing environment that is present now days more suitable would be complexes classification that combines several criteria for security threat classification.

But, even in these cases the use of to many different criteria, that are not interconnected in the proper way, and that are not dependable on each other would result with an classification that would be complex, even far more complex then necessary, but would not bring us any new information necessary for successful information system security management process.

Because of that we proposed a hybrid model for information system security threat classification, that we named *information system security threat cube classification* model or $C^3$ model. Te basic idea behind this model is to use the classification criteria that are necessary and useful. For this purpose we selected three main criteria:

1. *Security threat frequency* – a dynamically changing criteria that shows the frequency of security threat occurrence (e.g. how often is security threat executed);

2. *Area (or focus domain) of security threat activity* – what is the main focus domain of security threat? On which parts of information system it will act? This criteria is also a dynamical category and to avoid to large number of different focus domains defined by users, in $C^3$ model we are using predefine categories, like: physical security, personnel security, communication and data security, and operational security.
3. *Security threat source* – like in previous criteria we are using predefined categories, and the main division on just two type of security threat sources: insiders (persons, employees that are authorized system users that are using the system on daily bases for every day work assignments) and outsiders (persons that are not authorized system users). Inside each of these two categories is possible to create dynamical subcategories to satisfy the need for flexibility of the classification model.

The $C^3$ model is shown on the following picture.

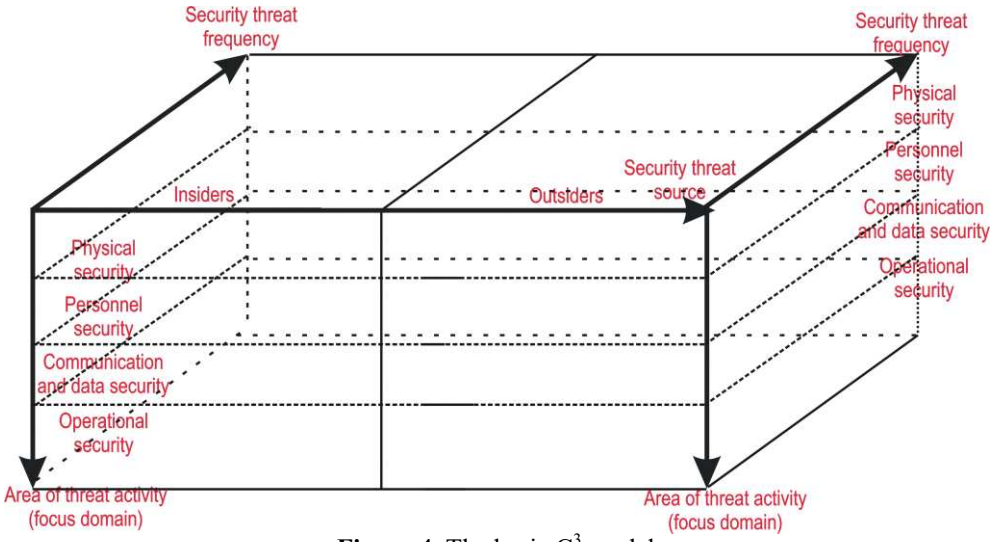


**Figure 4.** The basic $C^3$ model

To approve it, and to justify its structure we have place in it different types of security threats from classifications that were described previous in this article.

The next figure shows that it is possible to use the proposed model for different types of security threats.

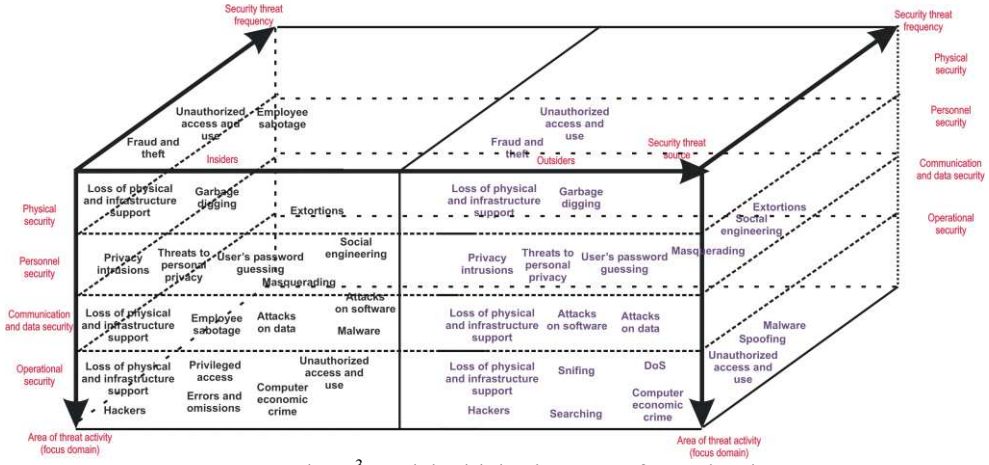


**Figure 5.** The $C^3$ model with basic types of security threats

## 4. CONCLUSION

One of the basic prerequisites for successful information system security management process is the use of certain security threat classification. Why? Because that way it is possible to determine from what we are protecting information system, it is possible to more efficiently use the limited resources (e.g. time, money, employees) by investing in those protective controls that are dealing with the most usual threats. That way we are indirectly increasing the level of information system security, and by eliminating the most common security threats more resources will be available for use on other areas of information system security. For that purposes we have to use some information system security threat classification. Existing classifications are being outdated, especially in context of their compatibility and comparability among them selves. To resolve this problem a proposed $C^3$ model can be used. It main characteristics are that it is flexible, dynamical and multidimensional model what gives him certain advantage compared to other mentioned classification models.

## REFERENCES

[1] Bača, M.: Uvod u računalnu sigurnost, Narodne novine, Zagreb, 2004.

[2] Denning D. E.: An intrusion-detection model, IEEE transactions on software engineering, Vol. Se-13, No. 2, 1987, <http://www.cs.ucsb.edu/> , (02.11.2004)

[3] Dragičević, D., Kompjuterski kriminalitet i informacijski sustavi, IBS, Zagreb, 2004.

[4] McHugh J.: Intrusion and Intrusion Detection, CERT Coordination Center,Software Engineering Institute, Carnegie Mellon University, Pittsburgh, 2001. <http://www.cert.org>, (12.01.2005.)

[5] ***: Arnaud de Borchgrave i grupa autora: Cyber Threats and Information Security Meeting the 21st Century Challenge, CSIS, 2000., <http://www.csis.org/homeland/reports/>, (03.11.2004.)

[6] ***: BS 7799, Preparing for BS 7799 Certification, British Standard Institution, London, 1999.

[7] ***: BS 7799-2:2002, The Newly Revised part 2 of BS 7799, XiSEC, 2002. <http://www.xisec.com/>, (10.12.2004.)

[8] ***: DTI A Director's Guide: Information Security – Best practice measures for protecting your business, DTI, 2004., <http://www.dti.gov.uk/industries/information_security/downloads.html>, (02.07.2005)

[9] ***: Information Security Breaches Survey 2002., CII, 2001, <http://www.dti.gov.uk/cii/> (25.10.2004.)

[10] ***: ISO/IEC 17799:2005, CARNet CERT, 2005, <http://www.cert.hr/documents.php?lang=hr&page=1>, (15.09.2005.)

[11] ***: ISO/IEC 17799:2000, Code of practice for information security management, British Standard Institution, London, 2001.

[12] ***: ISSPCS The International Systems Security Professional Certification Scheme – Version 1., ISSPCS Development Team, 2004., <www.isspcs.org/tpkb/>, (30.03.2005.)

[13] ***: Malware programi, CARNet CERT, 2005, <http://www.cert.hr/documents.php?lang=hr&page=2>, (31.08.2005.)

[14] ***: NIST – An Introduction to Computer Security: The NIST Handbook, Special Publication 800-12, < http://ts.nist.gov/ts/htdocs/230/235/pubs.htm>, (08.06.2005.)

[15] ***: 8th Annual BSA Global Software Piracy Study, Trends in Software Piracy 1994-2002, <http://global.bsa.org/globalstudy/> (10.10.2005.)

[16] ***: http://www.cccure.org/Documents/HISM/

[17] ***: http://informationsecurity.techtarget.com/

[18] ***: http://www.issa.org

[19] ***: http://www.iso27001security.com/

**Received:** 05 March 2007

**Accepted:** 07 November 2007