Journal of
Applied
Business
Information
Systems

http://www.jabis.ro

Illegal Operations with IT Software and IT Devices

Oana CRETESCU*, Lavinia Roxana LUNGU**

*, ** Master Student at Master in Accounting and Corporate Information Systems, West University of Timisoara, Faculty of Economics and Business Administration, Timisoara, Romania

Abstract: *The advanced development in technology and the large scale usage of information systems has brought with it a series of risks; thus, the increasing dependency of economic agents, of public institutions, and also of individual users to the information systems makes them more and more vulnerable to the impact of cybercrime. Therefore, the cybercrime phenomenon appeared, because of which the information attacks like: skimming, phishing, cyber bullying and happy slapping, can be materialized. Electronic computers are not an attraction just for the ones interested in development, but also to the ones only interested in gaining undue benefits from the usage of modern technology.*

Keywords: *Cybercrime, illegal access, interception, cyber fake, cyber fraud.*

1. INTRODUCTION

Cybercrime includes all offenses committed through the or with the help of computer, or computerized environment.

Regarding the concept of cybercrime, almost all specialists in this field, have tried to come up with a definition, but so far none of them succeeded so there is no way to tell how important or useful the definition is. Considering this, a functional approach of the subject is recommended, without the need for a formal definition, which can offer more difficulties than solutions [7].

Because functional approach was brought into question, it should be noted that this is specific to every state, thus, the facts bound to cybercrime are covered by the legal system.

2. INTERNATIONAL CYBERCRIME

Presently, new opportunities for breaking the law are offered, some of them being really “sophisticated” [6].

The transnational expansion of computer networks and access to these networks, through mobile phones, has led to an increase in information systems vulnerability, and also, to the opening of new ways of committing crimes.

Considering the fact that all social life fields (commercial activities, industrial activities, economic or government activities), are based on computerized systems, cyber technology has put its mark on individuals as well. Therefore, the daily activity of a person is affected by a computer in form, time and content, computers becoming a part of every individual personal life.
Presently, impressive amounts of data can be compressed and store on different devices, working speed has increased substantially, and the minimization of processors has made global real time communication and connection possible.

The fact that crime processing level in the IT field has increased is a certainty and also a challenge to every country in the world. Global level state legislation is in a continue state of change, which is due to the accelerated development of information technology.

Due to the increase in transnational cybercrime, international cooperation is in a continue challenge. More and more states have voted in favor of harmonizing their legislations in order to stop the cybercrime phenomenon, but for now this phenomenon is still active.

Maxim Dobrinoiu presents, in one of his works, the issues that are discussed nationwide regarding the overcoming of cybercrime [1],[3] :

- The absence of a cybercrime definition, accepted nationwide;
- The absence of a nationwide agreement regarding the motivation of such acts;
- The absence of expertise from authorized persons belonging to field control institutions;
- Nonexistent appropriate legal rules on access and investigation of information systems, including the nonexistent rules regarding the confiscation of computerized databases;
- The absence of harmonized legislation on field investigation;
- Transnational character of this type of crime;
- The existence of a small number of international treaties on extradition and mutual assistance in the field.

Among the first international organizations to mention the harmonized legislation issue in the field was Organization for Economic Co-operation and Development (OECD).

OECD published in 1983 a report which was addressed to all EU members. The report contained legal recommendations and a list of activities which should be punished: fraud and forgery by the means of computer, alteration of data, the interception of computer communication, copyright and access and unauthorized use of a computer [3],[9].

In order to complete the report published by OECD, the Council of Europe started own approaches concerning the realization of an own case study with the purpose of developing the legal way of fighting cybercrime. Consequently, the cybercrime field experts Commission of the Council adopted the R (89) 9 Recommendation, which is an action guide for all EU members.

Also United Nation got involved in the study for overcoming the analyzed phenomenon by publishing numerous documents, amongst which the most important are the following: „Propositions on concentrating nationwide actions on overcoming any form of criminal activity”(1985), „United Nation declaration on the base principals of justice regarding the victims of crime and power abuse”(1990), „Challenge without borders: Cybercrime- nationwide efforts for overcoming organized transnational crime”(2000).

3. CYBERCRIME TODAY

Cyber technology revolution led to fundamental changes in society, but one of the effects of this progress is the impact over the evolution of telecommunications themselves.

Classical communication, through telephones, was exceeded by the new methods of long distance transmission, not only of voice, but also of music, photography or film data.

Thus, it can be seen the fact that using electronic mail or accessing web pages through internet represents just a small part of the examples of this evolution, bringing major changes to present society, reaching up to the emergence of new crimes or to the committing of old crimes through the new technology. Therefore the existing legal concepts are put to the test, because in the last few years the Romanian legislator was preoccupied by the development of a normative framework which regulates the access and conduct of activities through information systems in different sectors [11].

In terms of history, more than 15 years ago, there was a worldwide attempt to categorize the social dangers of IT nature, grouped in „Computer Aided” category from which the IT acronyms: CAD, CAM, CAE, CASE, are part of.

Eight years ago appeared also in Romania the first law which reference certain offenses of IT nature. It is the Law nr.8/1996, known as the copyright law, which states among others, the protection of computer software author rights.

Nevertheless enough imperfections of this law were found, which combined with the faulty customs law have contributed decisively to the absence of and ending to court actions.

Thus, in the Law nr.161/2003 regarding the measurements to assure transparency and public dignity, as well as preventing and sanctioning corruption, there could be found three categories of crime [10]:

1) Crime against data and information systems integrity and confidentiality:

- the crime of illegal accessing an information system;
- the crime of illegal interception of data transmissions;
- the crime of alteration of data integrity;
- the crime of disturbing information systems functionality;
- the crime of making illegal operations with the help of computing devices or software.

2) Cybercrime:

- IT fake crime;
- IT fraud crime;

3) Infant pornography through information systems.

4. CRIME AGAINST DATA AND INFORMATION SYSTEMS INTEGRITY AND CONFIDENTIALITY

4.1. The crime of illegal accessing an information system

Illegal accessing an information system consists of an „interaction” between the perpetrator and the computing technique, through the components or through the various features of the „target” system (power button, mouse, keyboard, joystick, power source) [1],[3]. By manipulating such devices, requests are sent to CPU, which will process data or run programs for the intruder.
It is considered simple form illegal access when the intruder, using his/hers own remote equipment, finds and uses an external way to access another computer.

In order to obtain access to an information system, the perpetrator may use a wide range of technical procedures, for example: free access attack, exploiting the technological weaknesses attack, attack through password, TCP defalcation attack, etc.; these are just a part of the wide range of possibilities.

4.2. The crime of illegal interception of data transmissions

According to technical definition, interception means „the action of capturing, with the help of a special electronic device or with the help of computer, electric impulses, voltage variations or electromagnetic emissions which travel inside an information system or manifest as a result of a functioning system or are placed on a connecting route between two or more communicating information systems” [1],[3].

In order to prevent this type of attack, through network interception, system administrators use identification scheme, such as an on-time password system or a ticket authentication system (like Kerberos).

Generally speaking, a device or a computer can position itself in any point of an information system or a computer network. The purpose is to intercept message communication.

This type of attacks can have two forms: passive or active attacks. Passive attacks assume that the intruder just „assists” the transmitted information and does not interfere with the flow or the content of the messages. On the other hand, active attacks assume that the intruder steals or modifies messages, or is transmitting fake messages.

4.3. The crime of alteration of data integrity

This crime can be committed through multiple alternative actions which presume the modification, deletion, damage data, or even more, restricting access to data or unauthorized data transfers.

Modifying data means that the perpetrator may introduce new sequences or may delete specified parts of data [1], [3]. The result consists in obtaining new data, different than the previous ones and inconsistent with the truth before the modification.

Deletion represent the action of partial or total elimination of the binary representation of the targeted data, which is stored on Hard-Disk, CD, memory stick, etc. thus leading to the disappearance of respective data.

Damage consists in the distortion of data of binary content, through controlled or uncontrolled introduction of „0” and „1” sequences. Due to this, the new obtained sequence cannot have a logical counterpart in reality.

Restricting access to data is a result of the operation on computing systems or storing environments, through actions taken by the perpetrator. Therefore, the set problem is restricting access when authorized persons cannot use the data.

By the operation of unauthorized transfer it is understood the „moving without right" of the binary representation corresponding to the information from the authorized stored environment to another storage media, external or internal but in another location.

All actions by the means of which data integrity alteration crime is committed bring about negative effects towards data, especially their capacity to function in the manner intended by the owner.

4.4. The crime of disturbing information systems functionality

This type of crime can be committed through any action of serious disturbance of an information system functionality [1],[3].

In the legislative text content there are mentioned even the ways to commit the crime: „introduction, transmission, modification, deletion, damage or by restricting the access to data".

4.5. The crime of making illegal operations with the help of computing devices or software

This type of crime consist in the action of producing, selling, importing, distributing, or making one or more devices or software programs specially designed or adapted available with the purpose of committing a cybercrime.

5. CYBERCRIME

5.1. IT fake crime

According to nowadays legislation, IT fake is defined as "the deed of unauthorized introduction, modification or deletion of data, or unauthorized restriction, if the deed results in obtaining false data, with the purpose of using them in order to produce legal consequences".

5.2. IT fraud crime

IT fraud is realized through an alternative action of introducing, modifying, deleting data, or restricting access to the respective data or to obstruct by any means the functionality of an information system.
IT fraud is committed only directly, in order to obtain a material benefit for oneself or others.

5.3. Child pornography through information systems

When it is talked about infant pornography, this crime can be dined as „producing for spreading, offering or making available, spreading or transmitting, obtaining for oneself or others, of child pornography through information systems or possessing, without right, child pornography in an information system or media storage device" [1], [3].

This type of crime is found at the limit between crimes committed with the help of information systems and crimes committed through information systems.

Observing trends in recent years, the danger of child pornography „acts", using information systems, has increased significantly. Having this context in mind, the law enforcer imposed a special regime of incriminating and sanctioning this type of crime.

What is more, the data package interception phenomenon represents one of the most difficult crimes to commit, becoming a serious threat to communications over the internet.

Every package sent via Internet can transit numerous computers or networks before it reaches its destination. Thus, by the means of a package interceptor, hackers can obtain these data (including login messages, credit card numbers, e-mail packages), which „travel" between two Internet locations. After this process is finished, the hacker can open the package and steal the name of the host, the usernames and passwords of the accounts.

An interesting fact is that hackers use one of the most common type of package interception before an IP attack. Security experts named this type of interception as „network snooping" or „promiscuous monitoring".

In order to prevent interception attacks towards distributed networks, system admins must use identification schemes like on-time password systems or a ticket authentification system like Kerberos.

Although both on-time password systems and Kerberos systems can make the interception of an unsecured network harder, for any hacker both methods are exposed to active attacks if they do not crypt and sign the data flow [2].

Starting from the type of cyber attacks, passive and active, the four most representative are: skimming, phishing, cyber bullying and happy slapping.

5.4. Skimming

This method of obtaining credit card data has its origins in Asia. Between 1993 and 1994, the counterfeiters from Asia started to codify a three digit number in the unrestricted data field on the magnetic band of counterfeit cards to simulate the existence of CVC or CVV code.

The first case of skimming was reported in 1994, in a Singapore night club, and in the mid-90', the phenomenon extended to Malaysia, Hong Kong, Taiwan, Japan, indicating the prolific spread of skimming in Asian country territories.

The action itself presumes a series of facts that, individually analyzed show, on one hand the existence of distinct crimes, and on the other hand surprisingly that nowadays legislation in one step behind these „antisocial behaviors".
Presently, it is one of the most talked about crime regarding the electronic payment instruments and ATM-s.

Also, skimming is the way to obtain information about a card or a PIN code, through a „lightning attack". For example, a faction created thousands of fake cards, and then its members travelled to different cities where they withdrawn small amounts of money from different accounts so that the protection software could not detect them.

Skimming devices can be classified in hand skimmers and ATM/POS skimmers. The latest ones can be categorized in slot skimmers, installed on the card introduction slot, and door skimmers, installed at the card access devices in a bank entrance [4].

Until recently, the skimming equipment was pretty rudimentary – a device that was attached using duct tape or foam to an ATM's card reader, and small cameras for capturing the moment when a user introduced his/hers PIN code. Nowadays though, the equipment includes tiny devices, which can fit in a card reader, very small cameras or objects that look almost identical to the ATM's card reader or keyboard, and are placed over them. Nevertheless, bank customers are no longer defenseless in front of information thieves, because new technologies were developed to prevent data from being skimmed. One of these technologies is the new „chip and PIN" card which includes chips for a better protection.

5.5. Phishing

Phishing is a fraudulent process by the means of which it is attempted to obtain information, usernames, passwords, credit card details, or any other personal data through a message in which the author is presumed as a trusted entity [5].
The essential fact is that in the majority of cases the electronic communications come from banking sites, auctioning site, and online payment sites.

Usually, phishing is performed through the sending of instant messages or e-mails, by which it is demanded that users introduce personal data, and then they are redirected to a fake website which looks almost exactly as the legit website.

„The authors" use spam-like emails to direct their victims, amongst the most visited websites are the e-commerce sites. These have developed the phishing techniques and methods through the use of malicious cards, hidden in photo files or in web applications, and which install phantom applications, activated immediately.

5.6. Cyber bullying

Another type of threat is cyber bullying, which is strictly related to the aggression or humiliation of children through the use of technology. This crime can be committed through e-mail, text messages or instant messages.

It is worth mentioning that in the online environment aggression can mean much more: threat messages, uploading another child’s photos on pornographic sites, using the e-mail account, password theft and account lockdown, sending messages in another child’s name, posting personal or false information on blogs with the purpose of affecting another child’s reputation, the spreading of viruses, subscribing other children to pornographic sites.

Most of the time, victims of the cyber bullying become offenders themselves as a reaction to the injustice they had suffered.

5.7. Happy slapping

Considering all types of threats, the biggest social impact is generated by happy slapping which is described as an unexpected attack towards a victim, while a friend of the offender is recording what is happening – obviously using a mobile phone camera – in order to distribute or watch the record repeatedly.

Despite the name of the phenomenon, the aggression generated by it is not only slaps or physical abuse.

Presently, it has come to the recording of any type of molestation, which in some cases had unpleasant endings.

The majority of cyber bullying types are „one on one” aggressions, in other words, the offender attacks the same person every time. On the contrary, in the case of happy slapping, at least two offenders appear, as one of them has to record the other one’s aggression. This collaboration hurts the victim even deeper, because he/she perceives a bigger number of aggressions, consequently a smaller chance of resolving the problem by himself/herself.

6. CYBERCRIME ANALYSIS

6.1. Worldwide

Regarding cybercrime, worldwide, it can be said that Italy generates the biggest number of cybercrimes in the world, although in 2007 U.S.A held the first place.

Another fact worth mentioning is that at least one third of the cyber attacks were made from an American computing system.

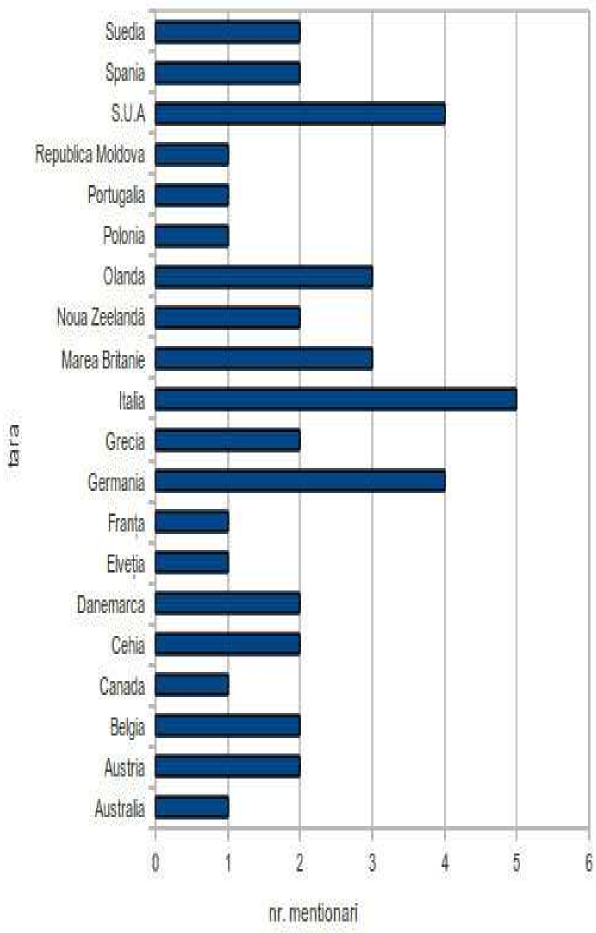

Figure 1. Cybercrime rankings by countries

6.2. Romania study case

In the year 2011 phishing attacks have increased (over 48.000 new threats) and in Romania, the main intention was to obtain personal data, passwords, credit cards, PIN.
On the other hand, IT threats, in the first three months of the same year have reached 13% of the total infections in Romania. Therefore, it was noticed that auto run type threats use the functionality of peripheral storage media and in this respect the Autorun and Sality factions follow-growing with three representants each.

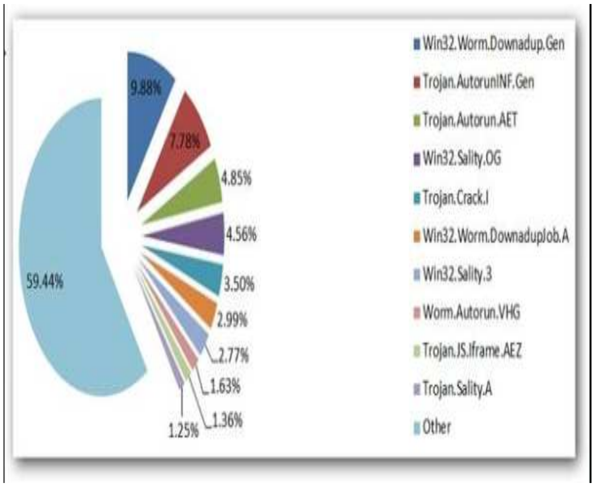

Figure 2. The top of cyber threats

7. CONCLUSIONS

After analyzing the four types of cyber attacks, the most dangerous for human integrity are cyber bullying and happy slapping, because they exceed the idea of individual intimacy „violation" by far or in the conditions of a so-called modern society that heads towards a new era, the one of IT „slavery", ignorance is a too high price to pay in front of freedom.

Therefore, in order to take action against such threats, the role of criminal groups resumes for the moment to the identification of some primordial elements:

- The obtaining of a substantial financial product and the targeting of payment systems offered by financial institutions;
- The organization of the acting groups, their structure and the specialization of their members;
- The usage of young people with advanced computer abilities, who are coordinated by criminal groups leaders;
- The transition from IT fraud, in which confidence was key, to frauds in which dominates the usage of computer software;
- The transactional nature of these deeds, in the sense that the crimes are committed from states different than the ones from which the victims are;
- The permanent preoccupation for identifying the products that can be frauded;
- The locating of the offenders on attack types and on destination countries.

Today it is certain that the computer has become the most popular instrument of fraud and forgery.

REFERENCES

[1] Amza T.- Criminalitatea informatică, Editura Lumina Lex, Bucureşti, 2003

[2] Bird L.- Internet-Ghid complet de utilizare, Editura Corint, Bucureşti, 2004

[3] Dobrinoiu M., Infracţiuni în domeniul informatic, Bucureşti, 2006

[4] Dobrinoiu M.- Operaţiuni ilegale cu programe informatice (WORKSHOP CRIMINALITATE INFORMATICĂ-TG.JIU, 21 IUNIE 2010)

[5] Rosario Ortega, Joaquin A. Mora, Merchan and Thomas Jager- Luptând împotriva agresiunii şi violenţei în şcoală. Rolul mass- mediei, al autorităţilor locale şi al Internet-ului (ARTICOL)

[6] Art.46 Legea criminalităţii informatice

[7]*** http://www.euroavocatura.ro, accessed at 18.05.2011

[8]*** http://www.LibrariaAtlas.ro, accessed at 30.04.2011

[9]*** http://www.internews.ro, accessed at 30.04.2011

[10]*** http://e-crime.ro/ecrime/site/index.php/materiale_documentare/hw_sw_ilegale/, accessed at 29.05.2011

[11]*** http://www.wikipedia.com, accessed at 28.05.2011

[12]***http://stiri.criminalitate.info, accessed at 04.06.2011

[13]*** http://www.securitate.ro, accessed at 04.06.2011