International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471
Vol. 3 Issue 5, May-2014, pp: (22-29), Impact Factor: 1.147, Available online at: www.erpublications.com

Lack of Data Security and its Impact on Economy and Government

Ali Aljafori[1], Ibrahim Jaluta[2]
[12]Department of Computer Science, University of Tripoli, Libya

Abstract: The development the world has witnessed in the last two decades of the last century in various fields has been accompanied by development in the communication technology. The result of which was the emergence of the Internet (International Network of Information). This twentieth century marvel has spread spectacularly around the world. The world has become almost entirely dependent on the continued availability, accuracy and confidentiality provided by the internet through Information and Communications Technology (ICT). In this paper we explore the world of security, protection of information stored or transmitted on computer networks, the methods used to support security and the how lack of data security can adversely affect the economy and endanger government control and even state sovereignty.

Keywords: Information security; Communications; Hackers; lack of security; ICT; sovereignty.

I. INTRODUCTION

In ancient times only few people were privileged with the ability to read. So a written text may be considered a secret unless it ends up in the hands of someone who can read. Because of that data security was not an issue. At least one case in history is known of someone who carried his own death sentence without knowing that. As the number of people who can read started to increase, the desire to look for better ways to protect the secrets started to increase as well. That became evident in war times.

Encryption methods started to appear in the exchange of Military information to hide the plans and armies' movements from the eyes of their enemies. Humans' need to communicate and the need to encrypt communication goes hand in hand. ICT has helped the use of more and more complex encryption techniques.

The first attempts to communicate came through the building of local area networks in 1964 to facilitate the sharing of information and services with the immediate surroundings. Soon after, began the development of wide area networks to provide communication and secure networking with larger groups. Wide Area Networks (WAN) appeared in 1966. It was the beginning of a new phase in networking revolution which had no limits and was able to transform the planet Earth to a small village or what has been termed the "Global Village".

The computers are "force multipliers" for those who use it. It Increases strength exponentially either as benefit or as harm. It is estimated that the number of devices used worldwide is increasing at a rate of 50% annually. Computing is crucial to the infrastructure of advanced countries. Yet, as fast as the world's computing infrastructure is growing, security vulnerabilities within it are growing faster still. The security situation is deteriorating, and that deterioration compounds when nearly all computers in the hands of end users rely on a single operating system subject to the same vulnerabilities the world over [4].

II. SECURITY IN THE INTERNATIONAL NETWORK

In this digital age that we live in and work, the individual as well as the institution finds that the information technology tools and instruments are indispensable in the daily work. Most modern societies have become almost entirely dependent on the continued availability, accuracy and confidentiality of its Information and Communications Technology (ICT). But estimates of the cost of cyber crime have until now failed to address the breadth of the problem and have not been able to provide a justifiable estimate of economic impact. Here the term "cyber crime" is used to mean the illegal activities undertaken by criminals for financial gain. Such activities exploit vulnerabilities in the use of the internet and other electronic systems to illicitly access or attack information and services used by citizens, business and the Government. In a study done in the UK, it is estimated that cyber crime is costing the country 27bn pounds per year. Study shows that cyber crime has a considerable impact on citizens and the Government. The ease of access to and relative anonymity provided by ICT lowers the risk of being caught while making crimes straightforward to conduct [14]. At the same time, the number of individuals and institutions who are exposed to security breaches in their information systems is on the rise. As networks grow and become increasingly complex, the risk of holes in security due to configuration and/or design mistakes increases. As increasingly more business critical applications rely on the availability of the networks; the exposure to loss is also becoming drastically higher [6].

III. CYBER CRIMES AND THREATS

Cyber crime is one of the fastest growing areas of crime. More and more criminals are exploiting the speed, convenience and anonymity that modern technologies offer in order to commit a diverse range of criminal activities.

These include attacks against computer data and systems, identity theft, the distribution of child sexual abuse images, internet auction fraud, the penetration of online financial services, as well as the deployment of viruses, botnets, and various email scams such as phishing.

Unlike conventional crimes of theft, in which the owner actually loses their physical property, the theft of information by cyber criminals may not result in the loss of anything physical at all. Moreover, the 'theft' can often leave the original data exactly where it was to begin with.

The global nature of the Internet has allowed criminals to commit almost any illegal activity anywhere in the world, making it essential for all countries to adapt their domestic offline controls to cover crimes carried out in cyberspace. The use of the Internet by terrorists, particularly for recruitment and the incitement of radicalization, poses a serious threat to national and international security [12].

A. Recent examples of Cyber Threats

Stuxnet worm (July 2010) - The Stuxnet worm (a complex computer code) was used in the first cyber attack specifically targeting industrial control systems. This attack seemed to be directed at Iran, and its nuclear programme. Stuxnet is unprecedented in its design to allow hackers to manipulate real-world equipment without operators knowing. The worm targeted Siemens' systems, used in the energy sector to control nuclear and gas infrastructure and also in manufacturing and automotive industries. Experts estimate that it took five to ten people to work on the Stuxnet worm for six months. The complexity and access to systems involved indicated a highly organised and well-funded project. The European Network and Information Security Agency (ENISA) has called it a "paradigm shift" in cyber threat [5].

Large scale fraud (2009/10) - An Essex-based gang, linked to Eastern Europe, was prosecuted for an on-line fraud making £2 million a month by stealing log-in details from 600 UK bank accounts and tricking users into providing additional information. The Police e-Crime Unit, working with the banking sector, detected the fraud which targeted weak security on individual's computers using Zeus Trojan malware (i.e. a malicious computer programme disguised as something else such as an email attachment).The fraud was co-ordinated from a single laptop with sophisticated software available on the internet [13].

Conficker (2008) - A botnet (A group of computers compromised and co-opted by an 'intruder'.) on an unprecedented scale has been operating since November 2008 affecting millions of computers worldwide using the Windows operating system [9].

The source of this threat is the permanent connection to the internet and the vulnerability of these technologies to be infected with these attacks. The origin of these damages may be electronic such as viruses, or it may be social such as stealing actual computer components, storage media for example. It is unfortunate that many of those exposed to such risks are unaware of it. Perception does not occur until after damage has occurred, which may often be costly.

For example, computer viruses' effects may not appear until after a specified period of time, and it may cause a difficult or un-repairable damage to storage media. The process of data recovery in such cases would be hard and very costly. The three main elements in data security are confidentiality, integrity and availability, symbolically known as (CIA).

IV. CURRENT SITUATION

Nowadays the information of most companies and institutions is in electronic form for ease of processing, search and exchange. The jobs related to the field of information technology requires most of the time the use of local networks and/or the Internet. For that reason, protecting information to achieve the three fundamentals of information security mentioned above is an essential goal for any organization or individual who uses this technology in his daily activities. These jobs often require the use of local area networks or Internet, so protection of this information to achieve the three foundations is an essential goal for any organization or individual who uses this technology in his daily activities.

Information security system that achieves these objectives achieves in addition non-repudiation and authentication. So the problem is summed up in the following points:

1. That civilized societies could no longer carry out their functions without the use of computers.
2. Computer networks multiply the force resulting from the sum of the individual computers (Synergy).
3. The network is the platform from which the hacker attacks.
4. Dangers threatening the security of information increase primarily on non-specialist users.

As noted, the civilized societies depend for most activities on the use of computers. Power systems, food distribution systems, air traffic control, banking, telecommunication and emergency services are just few examples of services that rely completely on computers to deliver the service.

The Internet, which was the product of a military research project to connect several computer systems geographically distributed at several locations in the United States, today covers the globe and contain many computer

networks, that include among them millions of computers. At the end of the eighties decade of the last century, it was 600,000 computers that rose to 36 million after ten years then to more than 171 million in year 2003. The number has surpassed 1 billion in 2008 according to Gartner, expected to reach 2 billion in 2014 [8].

Due to the size of the spread of the Internet and the low cost of use, daily business for individuals, corporations, banks and governments has become almost fully dependant on it. But the Internet and its communication protocol (TCP/IP) is not safe. The threats from the internet combined with loose or inefficient security policies, can cause the loss of sensitive and critical data. For government agencies and businesses backing up data is the best defence against data loss. A business that fails to maintain a copy of its data is asking for trouble. It is extremely easy to lose data and almost impossible to rebuild that data if backups don't exist.

A business without a backup and recovery strategy is asking for trouble and taking an unnecessary risk. IT staff should never allow this to happen. There are no excuses; backups should be given as much importance as the overall protection of the organization's network.

V. THE ECONOMIC IMPACT OF LACK OF SECURITY

Two recent studies found considerable evidence that the computer, or more generally IT equipment, is behind most of the recent acceleration in productivity growth [15].

The costs associated with cyber-attacks can be divided into direct and indirect costs. Direct costs include the expenses incurred in restoring a computer system to its original, pre-attack state. Another direct cost is the lost business revenue.
Attacks also have indirect costs, which may continue to accrue after the immediate damage has been repaired. Many indirect costs flow from loss of reputation, or damage to a firm's brand.

A central issue, in both public and private sectors, is whether we are devoting enough resources to information security. Part of the answer must come from economic analysis. What are the costs, both historical and potential, of security breaches? How frequently can attacks be expected? Can these factors be quantified precisely, so that organizations can determine the optimal amount to spend on information security and measure the effectiveness of that spending?

Several computer security consulting firms produce estimates of total worldwide losses attributable to virus and worm attacks and to hostile digital acts in general. The 2003 loss estimates by these firms range from $13 billion (worms and viruses only) to $226 billion (for all forms of overt attacks). The reliability of these estimates is often challenged; it is believed that actual losses are significantly higher. [15]

Not all incidents of data security breaches and data losses are reported. Organizations have real economic incentives not to reveal such information. The costs of public disclosure may take several forms:

1. **Financial market impacts.**
The stock and credit markets and bond rating firms may react to security breach announcements. Negative reactions raise the cost of capital to reporting firms. Even firms that are privately held, and not active in public securities markets, may be adversely affected if banks and other lenders judge them to be more risky than previously thought.

2. **Reputation or confidence effects.**
Negative publicity may damage a reporting firm's reputation or brand, or cause customers to lose confidence. These effects may give commercial rivals a competitive advantage.

3. **Litigation concerns**
If an organization reports a security breach, investors, customers, or other stakeholders may use the courts to seek recovery of damages. If the organization has been open in the past about previous incidents, plaintiffs may allege a pattern of negligence.

4. **Liability concerns**
Officials of a firm or organization may face sanctions under government laws if they are required to meet certain standards for safeguarding customer and patient records.

5. **Signal to attackers**
A public announcement may alert hackers that an organization's cyber-defences are weak, and inspire further attacks.

6. **Job security**
IT personnel may fear for their jobs after an incident and seek to conceal the breach from senior management.

International Journal of Enhanced Research in Management & Computer Applications, ISSN: 2319-7471
Vol. 3 Issue 5, May-2014, pp: (22-29), Impact Factor: 1.147, Available online at: www.erpublications.com

VI. CAUSES OF DATA LOSS

According to [11], there are 6 common causes of data losses:

•Hardware Failure
•Human Error
•Software Corruption
•Computer Viruses
•Theft
•Hardware Destruction

The first three causes account for about 82% of the data losses experienced by business owners in the US [11], (see Figure 1 below).
The cost of data losses is significant to business owners. According to Dr. Smith's research, based on data available prior to 2003, businesses experienced a staggering number of 4.7 million incidents of data losses at a cost of $18.2 billion dollars, (see Table 1 below).

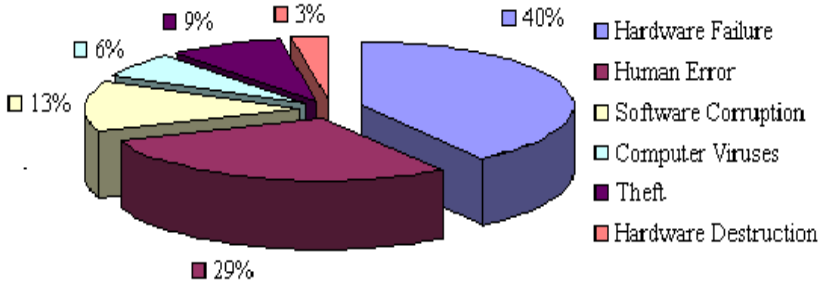

Figure 1. Causes of Data Loss [11]

Table 1: Causes and Episodes of Data Loss[11]

PCs in Use	**76.2 million**
Causes of Data Loss	**Episodes of Data Loss**
Hardware Failure	1,849,800
Human Error	1,345,300
Software Corruption	588,600
Computer Viruses	294,300
Theft	403,000
Hardware Destruction	126,100
Total	4,607,100

Although it is difficult to measure with precision the cost of lost data, and the analysis is sensitive to the assumptions that underlie its calculations, there are several reasons to believe that $18.2 billion is a conservative estimate.
However, there is evidence that individuals and firms alike are more likely than ever before to use power surge suppressors, UPS equipment and antivirus software. This improve the situation but it may be offset by the fact that more computers are on the network now more than ever before.

VII. WAYS TO ACHIEVE INFORMATION SECURITY

In a field study conducted by the FBI in 2006 about computers, it was found that [3]:

1. Viral attacks were at the top as cause of financial loss.
2. The unauthorized access to computer systems was ranked second.
3. That most of the institutions participating in the study gave significant importance to training to increase awareness of information security.
4. Toal loss as was found by this study in 2006 was more than 52 million dollars.

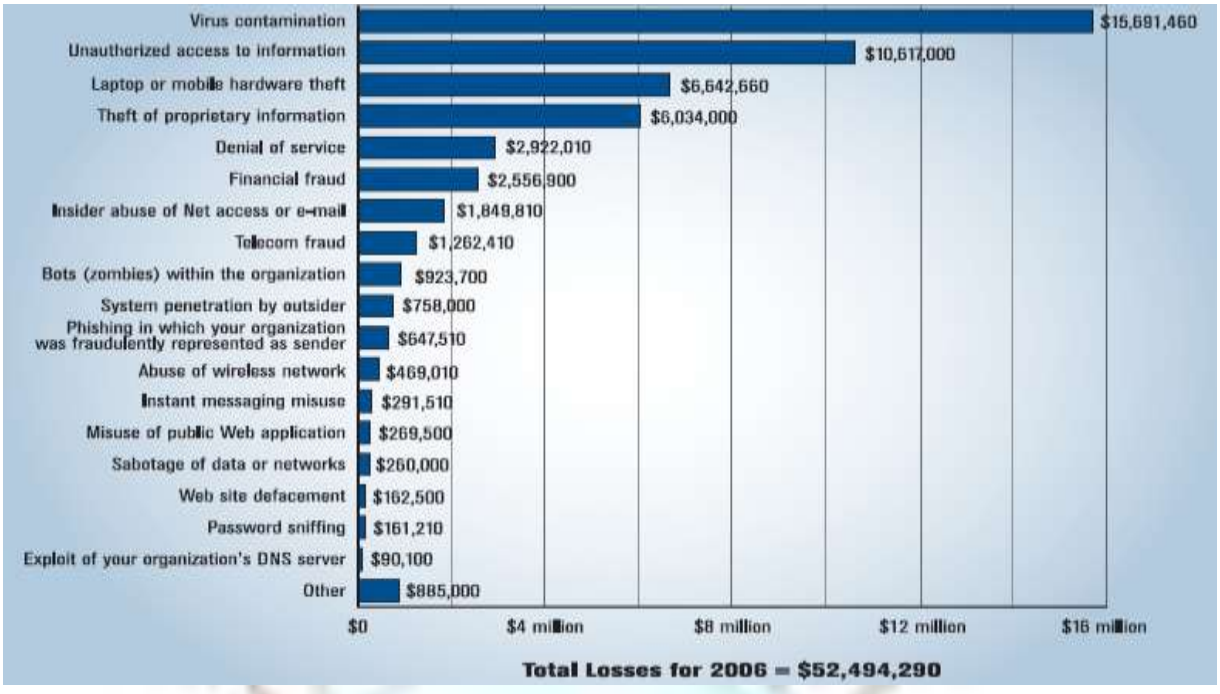

Figure 2. Dollar Amount Losses by type [3]

Therefore, the steps that must be taken in order to implement a successful policy to maintain the security of any enterprise information are summarized in the following points:

- Analyzing and assessing information security risks faced by the concerned institution and identifying their sources [10].
- The three security objectives of confidentiality, integrity and availability, i.e. maintaining the confidentiality of the information and making sure it is not altered by any unauthorized party and that permanent access to information should always be realized in the security system.
- Setting up the following technical and operational controls in place:

    1. Identifying the user and controlling the use of information. That requires the development of a methodology to identify the user unequivocally and assigning to each user (individual or group) his own rights of use.
    2. Verifying user authentication i.e. using passwords to make sure the user really is who he says he is.
    3. Maintaining the security of the system and its applications by diligently following and implementing these guidelines:

A. System Personnel

All administrators, operators, technicians and maintenance personnel of the system are expected to follow the instructions and information security policies stipulated by the foundation regulations. The management of the system must be assigned to a competent and knowledgeable person. He should be familiar with the technologies used in the system as whole and in particular the security systems used. He should be able to specify information security plans suitable for different components of the system and any other auxiliary systems, applications or data used.

B. Backup Storage and Retention

Backup and data retention policy should follow a careful routine for it to be effective and dependable. The following steps are basically what is needed [7].

- Decide what data needs to be backed up
- Decide where to keep the backup
- Store a full backup at another location or online to protect against fire, theft or other disaster
- Periodically update the backup
- Automate the backup process whenever possible
- Periodically test the integrity of the backup copy
- Always keep an updated log copy of the backup process.

C. **System Protection**

Action must be taken to identify and reduce access to computer systems and applications that contain vital and important system or institution data. Protect it from malware that use the network as a way to spread, such as viruses, worms and Trojans. Trojan and spyware ... etc., infect any computer or Server on the network, and usually cause the use up of the system resources resulting in a significantly slow system in terms of speed and performance. It can also destroy system resources such as the storage media or hinder network connection. It can also use the network to spread itself to devices on the network or to send a user's data to destinations without his consent.

D. **Privileged Access**

System administrators need a special permit to access the system that is not governed by the same laws normally governing public access. These include access to the system in non-working hours for maintenance purposes or system back- up or performance testing etc. This is called super user and is achieved through special accounts that can monitor activities of other user accounts.

Super user can do account creation, deletion or blocking and can change the password to any user account. For that reason, the persons with this authority must be trustworthy, and they should pledge in writing not to track or disclose personal or system data for system users whether obtained intentionally or accidentally.

E. **System and Application Software Development**

Organizations using computer systems must enact appropriate legislation governing the use of methodologies and rules of maintenance and development of these systems in order to ensure the achievement of the highest benefit of use. Must also be careful to respect and follow that legislation at all times by employees and third parties participating in the development processes, and work to improve and renew legislation and rules whenever the need arises.

F. **Maintaining Internal Security**

To maintain the internal network security major institutions with computer systems must apply special strategies to ensure user compliance with the requirements of the network. Firewalls, sensors, intrusion detection and prevention (IDS/IPS) must all be setup to strengthen protection and prevent denial of service attacks or any similar threats to the network. Resources containing important and critical information should be put behind firewalls.

The threat of attack from outside the company is real, and warrants significant concern and action from IT professionals. But massive data loss also results from internal activities. The insider threat is often characterized as an employee performing malicious behaviour through sabotage, stealing data or physical devices, or purposely leaking confidential information. Like outsider threats, addressing the insider threat demands a comprehensive approach that includes education, policy, and technology [2].

G. **Activity Logs**

In order to maintain the system integrity and credibility, any system change must be done according to a pre-set plan. In particular, any change to system essential and sensitive resources does not take place until proper authorization has been granted, and at the mean time keeping record of all changes made.

The change management process should include the following steps that represent monitoring and recording every change process:

- Monitoring and recording any changes made to the system.
- The necessary steps to track any changes that may have happened without a permit to do so.
- Ratification to carry out the test.
- Authorization to transfer application software from the testing stage to actual working stage.
- Tracking hardware equipment movement.
- Periodically examining the activity log file.
- Plans for Backup routines.
- User Training.

The activity logs that record the details of all operations of the system according to the actual chronological order in which they occurred is considered of paramount importance in monitoring the ins and outs operations of the system. They are also used in reading standards for the system use of sources and in identifying security threats and places of deficiencies. It also provides a reference of user activities that can be used when needed.

H. **Awareness Training**

In the above mentioned FBI field study respondents gave a high importance to security awareness training in the categories listed as shown in the figure below.

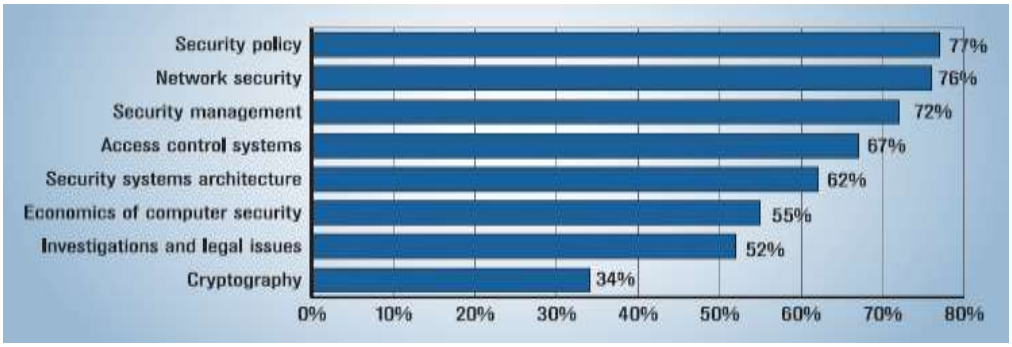

Figure 3. Importance of Security Awareness Training [3]

I. Use of Encryption

Strong encryption methods must be used whenever necessary for information in storage media or when sending it through the network. Highly important information should always be encrypted with the strongest encryption methods to protect it while transferred.

Encrypting data in storage should be used with extreme care, lest losing the key and losing data as a result. Therefore, the use of encryption, must take into account the nature of the information and the requirements of the institution concerned in terms of the information permanent availability.

Important information should be stored encrypted on portable storage media and kept in a safe place outside the site of the institution. As for the encryption keys, a specific plan must be used detailing how to reverse the encryption process and retrieve the data if keys are lost. That may require keeping a backup copy of the encryption keys.

The plan must also include a periodic review of the keys to make sure not to spill any of them to a third party. In addition, the Institution must also conduct a thorough search in career history of the people who are assigned the responsibility of managing the encryption keys, its software and hardware. And in particular, the plan must specify the encryption strategies in the following cases.

- Email
- Network Printing
- Remote file services
- Database access
- Communication interfaces between applications
- VPN
- Encrypting the entire fixed disk
- Encrypting a specific file
- Interactive sessions
- File Transfer
- Net-based applications

The British Standards Institution (www.bsi-global.com) and the International Organization for Standards (ISO) (www.iso.org) have suggested standards for practical application of information security which makes it easier for individuals and institutions to develop effective systems for the security of their information.
Furthermore, a successful policy must be independent of specific hardware and software decisions to adapt to changes in an agency's working and operational environment [1].
A suggested policy framework might be the following :

High-Level Organizational Policy	Standards, Guidelines, Processes and Procedures that Support the Policy
Asset Protection	Data classification, access control, personnel practices, change management, network security and disaster recovery
Vulnerability	Change management, wireless, vulnerability testing, application development
Threats	Incident management, penetration testing, audits, firewalls, malware prevention
Awareness	User education, IT education, annual certification, administrative rules
Appropriate Use	Education, Web filtering, content filtering, peer-to-peer, resource use for personal purposes (i.e., instant messaging, email, remote access, Internet, etc.)

CONCLUSION

The threats to information security have become a growing danger, given the breadth of the internet and the number of local area networks connected to it globally. What makes matters worse is that the majority of network users in the world are using computers running on the same operating system. This means that what affects a device may easily be transmitted to other devices. To protect against transmittable malware, antivirus software and firewalls are a must use. Private networks running different operating systems can also help limit the spread of malware, so infection can be contained. The old saying: "an ounce of prevention is worth a pound of cure" is translated to "Always backup data on a periodic and regular basis", and always test the backup and verify its integrity. Always keep the backup copies in a safe place away from the organization site. Physical security and personnel background check should be common practices in any organization, otherwise damages that may occur can be irreversible.

REFERENCES

[1]. California Office of Information Security and Privacy Protection. Information Security Program Guide for State Agencies. April 2008.
[2]. CISCO White Paper - C11-506224- 00 11/08 Data Leakage Worldwide: The High Cost of Insider Threats.
[3]. CSI/FBI Computer Crime and Security Survey 2006.
[4]. Cyber Insecurity: The cost of Monopoly-How the dominance of Microsoft's products poses a risk to security 2003.
[5]. ENISA Press Release, European Agency analysis of 'Stuxnet' malware – a paradigm shift in threats and Critical Infrastructure Protection, 21 October 2010.
[6]. Ericsson White Paper, 284 23-3075 Uen Rev A: Managing Network Security .
[7]. GFI White paper: The business implications of not having a backup strategy.
[8]. http://www.gartner.com/newsroom/id/703807.
[9]. http://en.wikipedia.org/wiki/Conficker.
[10]. http://www.interpol.int/Crime-areas/Cybercrime/Cybercrime.
[11]. http://gbr.pepperdine.edu/2010/08/the-cost-of-lost-data/.
[12]. Layton, Timothy P. Information Security: Design, Implementation, Measurement, and Compliance. Boca Raton, FL: Auerbach publications, 2007.
[13]. Metropolitan Police News Bulletin 1527 Gang sentenced for 'trojan' bank theft scam,16 November 2010.
[14]. The Cost of Cyber Crime./ A DETICA report in partnership with the office of Cyber Security and Information Assurance in the Cabinet Office.
[15]. The Economic Impact of Cyber-Attacks- Congressional Research Service ˜ The Library of Congress 2004 .