Nov 2nd, 4:00 PM - 4:15 PM

The development of IT and Telnet and its Impact in Business Security (non Security)

Musa Tahiraj
Post and Telecommunications of Kosova, uni10f@hotmail.com

The development of IT and Telnet and its Impact in Business Security (non Security)

Musa Tahiraj
Post and Telecommunications of Kosova
Email: uni10f@hotmail.com

Abstract. During the years, the people are more hungry for faster doing processes and works. There always is high possibility for loss business and markets by different attacks in different layers. In this paper is presented which are the challenges faced with information security on businesses during the rapid development IT and Telnet. This challenge requires stable technology, the standard platform and especially policies and rules for implementation security steps through those rapid changes in technology. In the paper are presented some of statistical review about the causes of information damage, which are advantages and weaknesses using new information technology. At the end is presented a model with seven attributes which has impact in information system security for every kind of the business.The paper has descriptive-narrative, statistical and inductive nature.

Keywords: Developing technologies, telnet security, computer threats, policies, rules

1 Introduction

The communication is old as the human bitch existing. For businesses is essentially the clear and effective communication. For faster and effective communication is necessary using the information technology. Using the newest information technology have consequences in increasing the risk in security. Using the equipment (computer, etc.) as intermediate medium for communications between the peoples or businesses is the reducing the time and money. Every information which is need for communications between individuals or between businesses, is done by calling through telephone; text and instant messages, e-mails (electronic mails); chatting or videoconferences. All this advances were used for faster delivery or exchange information, also for reducing money (paper, etc) and time. The other revolution in information technology is social media. With this kind of networking the people can communicate between them, and to post a comment about work or their life, make new friends, make new relationship with anyone from the used sites. Through websites present your business fields, communicate with your client online, e-buying, e-marketing.

Other advantages using and implementing new information technology is the calculations and processing different processes and services. In this point of view, today we have more applications in different area for drawing or plots, design or construction with tools.

Although there, exist many of advantages of using information technology, always is challenge the security of this information. When we talk about the security information, it means the security assets in physical and intellectual property. While the information must carry through a transmission medium, there always exist the risk for stealing, missing, violence, bad handling and deformation the same.

2 The history of development Information technology

The development of information technology is old as old or long has been discovered computers.
The computers are described from ENIAC by year 1940. Those computers are builder as series of machines by Harvard and Bell. During the most of years the computers are developed and transferred in machines and systems for easy handling information. The researchers and specialist has developing a many prototypes of computers and machines for handling and processing information by year 1970 and late. Many of computer museums were prepared and archived (Computer Museum in Boston, etc.)

The past two decades were a heaven activity about researches and development computers and information technology in generally. There, mostly of focuses and emphases were in discoveries and inventions in specialized fields and disciplines.

In other side, except the hardware development there were developed many software applications and operative systems in different fields of information technology and in different countries.

Today computers are using in many technical, medicine, social and economical contexts, in calculating, in handling and processing information the different nature and scope.

In 1981 IBM released Personal Computers. After this, was developed the mainframe computers for calculating the big data in shorter times. As its range of using those features has grown, the developing information technology was rapidly, so too difficulties are grown for understanding and controlling this rapid growth. Researches and experiments were made by many manufactures and developers in computer networking (ARPANET). Advanced research Projects Agency was created by the U.S .Department of Defense (DoD) in 1969 for reliable networking between universities and military research. After this is developed internet with high speed traffic. Last years is developed internet2 also called Next Generation Internet (NGI) with speed up to 2Gbps, and to transmit data at 100 Mbps.

Later in 1990 the computer industry has evolved in more complex and functional structure. The Microsoft and Intel has the power over market in the world.

Parallel with the hardware industry is developed and software industry (tracks are by year 1949).

"Computers (whether free standing or embedded in consumer electronics) have replaced

Record player, walk men, analog television receivers and videocassette recorders. Books, newspapers, and conventional telephones now appear endangered. In the office they have replaced typewriters, adding machines, bookkeeping and billing machines, duplicating machines, letters, memos and carbon paper. Videotext systems swept the western world.

File cabinets are vanishing, and in recent years the amount of paper used in American offices has finally begun to diminish. Computer networks are central to every kind of business operation, and play an increasingly vital role in our social lives and personal communication. Databases, automatic data capture, modeling, and statistical analysis capabilities have transformed practice in almost every area of science".

There exist many of operation systems such as: Windows (XP, Vista, 7,8, Mobile, Embedded); Mac OS; Mac OSX; Unix; Solaris; Linux; Red Hat Linux; Palm OS etc.

3 The advantages of using the information technology

The Computers become a very important kind of technology embedded in digital technology. This technology field named widely as information technology is a space for intellectual people who are interested in application of computer technology in interdisciplinary fields. In many fields have been applications microcontrollers-e electronic chips which are with memory and programmability available. In many enterprises and institutions are build the microprocessors (minicomputers), supercomputers, operating systems, computer communications, information systems or other types of virtually computers connected through networks. Networks are different types, depending in it how secure must be network – nature of security point of view, or how the enterprise is large and in geographical distance (LAN, MAN, WAN, International Networks, Mesh). In cases where request for security is very high, then equipments which are connected the between two ends is -VPN- modem. The last case often is used in banks or institutions where sensitive data are in high level of security. Although there have exist some kind of VPN-s equipment and kind of networks, the security is very challenge issue of integrity data and assets in enterprise. The other revolution in information technology is social media. . With this kind of networking the people can communicate between them, and to post a comment about work or their life, make new friends, make new relationship with anyone from the used sites. Advantages using and implementing new information technology is the calculations and processing different processes and services. In this point of view, today we have more applications in different area for drawing or plots, design or construction with tools. Applications are in schools in different area, in administration, in businesses. The other field of using the information technology is, in military use, in determine the climatic conditions, prediction the earthquakes.

The advantages implement the technology is in health (detection different viruses, ills), implementing in detection or finding DNA. Using DNA will help to solve the crime. Using finger print will help to find the thief or killer.
Today are developed many wireless communications protocols which are defined by the IEEE 802 series standards. In many countries in the world, is in use the 3G and Wireless Communications .This technology allow global roaming with a single handset. This standard provide 2-4 Mbps speed and enable VOIP mobile multimedia, video telephony and interactive gaming.
Also in testing and using is 4G Wireless Communications. This is named and LTE
Now days, the mobile telephony is developed faster more than ever. Emphases, is in equipment for end users. This is happen due to increase possibility for better and advanced communications.
Based in report by company for market research-IDC, the smart phones have exceeded the number in compare by simply phones, tablets expected to exceed the number in compare with personal computers. The delivery for tablets expected to exceed personal computers at the end of the year 2013, reported by IDC. This research company provided that this year will be sold 227.3 million units, until personal computers will achieve number of 315.3 million units (180.9 million from this number are laptops)
The smart phones expected to be sold 1 milliard units.
In the world are going deeply in improvement operation systems for phones in different platforms.
The new version of operation system by Google, Android 5.0 Key Lime Pie also will be a great success for Google which is ready to be released this autumn. This kind of operation system will be in able to work with older phones (phones which have no less than 512 MB RAM). In this case is very challenged issue how is security level when you not have enough memory for installing other security application?
In now days is present and news that in the future will be communications between smart phones without mobil network. Based on Telegrafi, soon will be communication smart phones without mobile network. It is possible by support or through named Project Serval, open software which will give possibility the smart phones to communicate with one each other without mobile network. Based on this paper or announcement the communication will be done through equipment which is similarly with router, through which will be access. Also in this chain every smart phone will be any equipment for connection with other mobile smart phones, creating the WI-Fi Network ("mesh" network), through the operative systems Google-Android. This application can be downloaded free. The new mobile application WeChat is known in Asia, soon will be distributed and in other part of world. It will be as substitution for applications by Face book Messenger, Skype, or Viber (Telegrafi.com /23.06.2013). This application is developed by Chinese company Tencent, which in China is known as Weixin. WeChat has and some other functions except messages and telephone calls, which are important for users (Time Magazine). This application is presented for the first time in public by year 2011, and has attract more than 400 million users /Telegrafi.com/. Viber is known program for "smart phone" users through which the call cen be done free.
(The example for loss profit impacted by Viber is PTK-Vala, where the inputs or profits in this company were less in this year for 12 million euro (Tribuna/Telegrafi.com).
This kind of technology implementation has impact in decreasing the number of employment in businesses which are working in telecommunication companies.
http\\: www.telegrafi.com (date 14.07.2013). The communication smart phones without mobile network will be soon.

4 The security (non security) business information

Every enterprise have sensitive data, regardless it is small or large enterprise. In many cases until the enterprise grows, there exist possibility for diverse or disparate organizations in security technology, approaches or accesses in work documentations, different policies etc. Those changes require more care about security assets and data. For organizations (institutions or enterprise) is very easy to secure physical assets, but for the data security is very complicate issue, regarding the rapid development information technology.
When there occurs security incident for enterprise is very difficult position, regarding the loss of productivity, loss of image, loss of commitment in competitive market.

With your data in enterprise you can communicate, relationship with customers, control of cash flow and economical and technical infrastructure.

When you are handling the sensitive data, it is unjustified to not protect data and care about their handling and by whom. There are possibility risk of managing the data anywhere, by people inside of the company, outside of company, and through transmit and receiving data. Every change or renew the policies and rules, new technologies, new people or different access in data must provide right secure information, with right people. The secure information means the secure business, to avoid risks by access the others in your data.

The key role in your IT data or in generally business data for your business is IT Manager or IT staff in your company. Until the company is small not necessary to have IT manger, but when your business grown, there need following the news about technology, about operative systems (OS), about updates, about antivirus program, antimalware and anti spyware programs for protecting your data.

In order to protect data by bad handling or missing data , you must coordinate the level of access for every employment, which is appointed for handling the data.

There also is very important keeping secure your PAN, LAN, MAN or WAN network. In order to protect data in use through MAN or WAN network there is very important using VPN connections. The challenge issue is to secure data in International Network and Mesh Networking.

In order to manipulate or store the data in right way, there are some of possibility to have attention in those:

- Which data would be break the company if they are lost or stolen (supply chain with relationships; e-commerce, e-banking, vital documentation for alone machine in production or services.)
- Which data would be dangerous in high level for company if they are lost or stolen(financial data, email (outlook) by different Internet Service Providers, intranet access)
- Which data are useful for product(processes) or services but not are critical for company (, sales, support desks, internal data for access, servers, supply chain, call centers)
- Which data are important for developing in the future in company.(research and development, supply chain, financial, portal, legal, marketing issues)
- Which data are important only for consumers, or for employment, not in generally.
- Types of special order (prescript) products, web servers, price in different countries with different level of market, price in huge amount, price for subcontractors etc.
- Which data are open for marketing issue.(all of this data aren't, important in time occurs , but for the future are sensitive depending by the way of their distributing, and in which media)

In order to avoid lost data or stolen, you must create a excellent information systems with clearly access for everyone and to have an updated operative Systems. Make protect for viruses (Antivirus program), make protect against spyware (or in generally Malware or Gray ware)

The very important issue for protection data through servers and other ends equipment is to keep in secrets , which type of server enterprise have, which kind of other equipment are installed and which are IP addresses.

Today is possibility to buy equipment by different manufacturers and by different countries. Very delicate is to select from who you buy some IT equipment or some electronic machines who are using software application. This stand is because you don't have knowledge about this software in which platform is used, or you have little knowledge about it. In this case is better to employ somebody who is suitable for this issue, and also contract training course with supplier.

In some cases the supplier have intention to stole data from your servers or computers. This intention often happen through selling Network Interface Cards (NIC) for computers. In this way exist possibility to be stolen your physical address of your equipment (computer),and then after a period to make access or attacks in sensitive data.

To avoid those things, your decision must take in consideration:

- Who is the supplier?;
- Which are relationships with his country and your country?
- Which are economic and political relationships between two countries?
- Which are your competitors and in which country they operate?
- Which are relationships between your competitors and your suppliers?

After those questions and answers from yourself (data collection), you will decide who is more responsible to supply you with the defined equipment (hardware) or software applications.
Of course this, which i remind above, is very crucial for medium or big enterprises, where the economic power and sensitive data is high. Except power in economical point of view there is very sensitive data when will exist very strong competitions in the market.
Another problem is storing data (create backup data), but in which place you save those data. Are this data stored in backups with standards and policies? Who have access in those data? All of those questions require answer.
Although you have some of the security attributes in enterprise, there always will exists the possibility for attack by hackers or cyber criminals.
The one kind of market in illegally is black market, in which goods and services are traded in ilegall form. The information technology in many cases help this kind of technology in preparing and implementing this market. Only in some cases the transfers or transactions coludn't be in
Illegal way. The black market is motived in order to avoid taxes, to trade contraband, or to avoid the price market. This is informal economy. This kind of black market often is discovered by using the information technology, through survivalience or through transaction. In some cases the advanced technology help this kind of market, based in fresh information by both seller and byer, for berhavior the government authority or other interest groups.

4.1 Viruses, Worms and Malware- a form of attacks?

The definition for Malware is done by many authors, one of them (Albert Road - Trusted Impact Pty Ltd.) has created this definition:
"Malware" is a general term for malicious software, and it is a growing problem on the Internet. Hackers install malware by exploiting security weaknesses on your Web server to gain access to your website. Malware includes everything from adware, which displays unwanted pop-up advertisements, to Trojan horses, which can help criminals steal confidential information, like online banking credentials.
For good protect by malware, you must take in consideration through your IT staff those actions:
In which way malware are distributing by hackers; which is profit of computer criminals infecting users; which are tools used for infecting those web servers (web pages)
Which are used techniques or developed techniques to infect more of websites, in which way the hackers distribute their code to infect websites, especially popular websites through malicious advertisements. The way in which the malware can be minimized is the using firewall through networks at each operation systems. The intention for malware is to spread viruses, attack the computers, steal sensitive data, credit card number etc. Malware in generally is distributed through Web browsers. In this context many of website from businesses are in risk hacked by malware

Some types of Malware are presented below:

- Software updates
- Banner ads
- Downloadable documents
- Man in the middle.
- DNS poisoning

Symantec is provider for security in management systems and storage, protecting against risk and enabling the information confidential.
In any enterprise is very important to make a information system which is stability and security.Based on relevant parameters in enterprise, you need to have solution for every section to predict the business risk. During the plan of information security is necessary integrity, confidentiality and availability information. Exchanging information between employers or between the contractors or subcontractors is very sensitive information. Based in the confidentiality those exchange information or reports must

be ensuring by other viewing. Only the people who are authorized can be conducted with those information and have access in this information.
The technical project or financial projects which are sensitive for a enterprise, must be confidential for most of people who are working in enterprise, not only for external people. The integrity of this data is very important issue based in entirety and accurate of this data.
Although the information system security is mainly technical issue, often the problems connected with security are as result of no correct handling the data by management or employment people. For this reason is required that people who handling the sensitive data, not only the sensitive, must be prepared and trained as policies and rules are required for a enterprise information system. Those policies and rules often are not prepared and not known as it enough must be. The level of knowledge for this policies and rules are and today the challenges for management and IT staff, especially for stakeholders which often not are informed or linked about it problems.
Although , every serious enterprise is prepared for security data through the some mechanism for control such is Updated operation system, Firewalls, Antivirus and Antispyware(Antimalware) programs ,data encryption, different backups, IDS, IPS, etc , it is not sufficient.
The interview with employment as IT administrator or IT manager, or in general managers, has result that , all of this controls are insufficient. *The many of those problems has derived by lack of understanding policies and rules for information systems. In other cases my opinion is that cybercriminals are working uninterrupted in infection and steal the sensitive data such are the credit card numbers, found transfers, e-commerce and other sensitive data. In sensitive data are included and technical specifications for different projects. In those specifications is possibility find who are the suppliers and which are capacities for product processes or services. Except those information in technical specification are included and technology processes which are vital for enterprise.*
All of those attacks by hackers or competitors are very danger for every business small or big.
Every business, especially banks and center for civil registration, must care about data integrity for business and customers. For customers sensitive issue is privacy for personal data-personally Identifiable Information (PII). Another sensitive data for customers is asset protection (account number in bank, credit card number , type and sum of transactions etc.)
The statistics has indicate that often this privacy is broken by employer of institutions or attacks by cybercriminals. Businesses which are licensed in any way they have legal framework defined by government in many facets, including and security of business. It not means that government is responsible for business attacks by hackers, but responsible for providing the secure environment for allowing and doing businesses. This is because the businesses pay different taxes for government. *In some cases the enterprises didn't know which are the policies and rules for information security and what is SLA (Service Legal Agreement). The SLA is important contract between businesses and any Service Provider for connecting in internet or in other Services.*
For security business is necessary to provide international security standards,
The ISO 2700 Series are standards which are developed International Standards Organization, providing a broad information security procedures and policies for all kinds of enterprises.
The main standard for this issue is standard ISOO 27001 (International Organization for Standardization) which is released for establish for ISMSS (Information Security Management Systems (ISMSS). This system is designed for planning, implementation, monitoring, and improvement information security.
NIST (National Institute of Standards and Technology) of the US is other standards which include a set of requirements (Special Publication -800 series) for increasing data security payment account. Other standard is PCI DSS – Payment Card Industry Data Security Standard.
For information program security is essential encryption, application security, recover data by disaster. Those security issue can't be done successfully without any good organization and managing the program security. There are possibility to organize the ***frameworks*** and rules for security program for every enterprise. This framework is contented by some documented processes where are defined the procedures, policies or rules for managing the risk in information system security and reduce the weaknesses in this system. One example of framework is COBIT (Control Objectives for Information and Related Technology) developed by ISACA.

How much are security those tools and standards there is a big challenge. Always must have improvement in technical aspects of control and avoiding manipulating the business data. Not only in technical view, but in organizing is very important to connect all management staff including and stakeholders. Important is a business strategy based in organizing departments and human resources in right way. It means everyone to have responsibility for their job, and everyone who have access in information system to have knowledge about privacy policies, rules and everything was changing. Everyone in his place with adequate of knowledge. For businesses who have implemented multiple technologies, is very key thing that people who are working within it to be independent and arbiter. In this case IT stuff should be neutral for each platform of services. How much dependent are employs doing business in different platform of technologies?

Internet is going to be more and more dark place for business and individuals.

Many books are written for antivirus and antispyware, but little of them or none explain the clearly the way of infection and hackers. It is not so for commercial issues, but it is for every day changing the situation and the cybercriminals are behind the government shadow.

The people or institutions which are responsible for protecting the attacks and infection by virus, spyware, malware etc, not are in correct level. The government must be more flexible about organizing Email from your inbox is the next story for business challenge.

Is the same thing when you receive a envelope paper written for you and send at you, and email from inbox? For many reasons no! Email often you read and when answer is not ready, maybe you forgot to answer , or mistake decide to delete this email. To be more efficiency with work flow, you must define the response time. Issue is that you should decide about important email,, important with need to take action, important but not urgent, and not important. To know how much is reliable and secure is backup and recovery system for any business, you must ensure the best practices for high quality backup data. The way how backup data is taken and how it is organized will be confidential for any enterprise. Did this happen always? The answer is no!

The backup data must be more ready for run if it is required, without any much need for interaction by administrators. This is very ease and comfortable for people who have knowledge about it.

Now days are possibility for data efficiency, maintenance in security issue etc.

In the world exists many companies which deal with the security business? One of them is ADT Pulse Most of this companies offer: Protection from burglary, Protection from robbery and intruders, Monitoring fees, Fast alarm response and more remotely control equipment, Arm/disarm your system, Video Surveillance, Electronic access control

Do you believe in any company for those security parameters? The answer is different and difficult from different people. If you wish to advance in your business or technology processes, you are forced willingly to be a part of this security.

4.2. DoS and DDoS

One form of the attack which prevents users from normal accessing services such as e-mail or web server is Denial of Service (DoS). This attacks is done through *ping of death* or through *e-mail bomb*

One the newest way attacks from hackers is Distributed denial of –service attack (DDoS).

This attack is created in such way that, they attach a single target creating a flood of incoming messages to the target system, make him to shut down, so denying services to the system by order users. This attack uses many infected computers which are called often zombias, and intention is to overwhelm access to the targeted server.

This issue is treated as the biggest threats to internet security.

Until now there are known two types of DDoS attacks: a network layer attack and application layer attack. For avoiding the DDoS attacks you should carefully implement optimum configuration the networks, make constant update and permanent control of elements to the systems.

Protection from DDoS and other attacks. *You must put the right people in right work place, it means everyone to be responsible and agility for his work. Those people must be trained in his work, regardless the number of employers an enterprise have. Work people in enterprise must have enough knowledge to use the technology to detect and minimize those attacks. Keeping emails under control, work efficiency and secure with application and operation systems, emphases in opening the susceptive and doubtful sites and links.*

An example of diversion or attack is San Francisko bank that was robbed of $900.000 during a DDoS (wrote by Warner).
DDoS are growing every day and are being danger in many aspects of attacks in high bandwidth volumetric attacks, especially in the cloud computing services. One good defense and protection by those attacks is On-Premise DDoS Protection especially in application - layer threats.

4.3. Some statistical review

Based in Symantec report, the Google are included in many scandals. The first scandal was the delivery secret information for FBA in America. The second scandal is the flowing secrets for telephone numbers and emails for 6 million users. In fact Face Book mobile application Android for smart phones, has a big issuance about security, because the same application automatically give the phone number social network Face Book in which is installed. After the publication this data by Symantec, the Google asked forgiveness and has premise that will delete those number. Do you believe in it?
In UK more than one –fifth firms hit by DDoS attacks in 2012, report wrote by Warwick Ashford

The poll of 380 IT professionals shows that DDoS attacks are threat to large and small organization in all sectors, yet many organizations do not have adequate protection in place.
Key industries reported the highest levels of attack, with53 % of telecoms firms, 50% of e-commerce business, and 43% of retailers reporting DDoS attacks. 37% of DDoS attacks reported lasted for more than 24 hours, 24% lasted for more than three days, and 22% lasted for more than a week. It is likely that more than 20% have practically no protection from DDoS attacks, even though they think they are protected .
Based in above mentions for DDoS, there is more important to take proceeding in avoiding this attack or to minimize. In different businesses exist the different ways for avoiding or minimize those attacks. Depending by firms size, and by capacity exchanging information there are possibility to put the especially policies for protection by attacks. Protection can be done in different way, but the same target for all is protecting data and privacy for business or individuals .
In question: "How Secure is Your Company" Prof Chi-Chun Lo, (National Chia-Tung University) has gives a good answer:
"One foot in ice water and one foot in boiling water does not mean that on average you are at room temperature.

- Corporations are not monolithic, and all parts of the business don't have (or necessarily need)the same level of security.
- Security is not an end state, nor can it be judged by measuring any single variable at any single point in time."

For Security as a service Bill Malick Gartner has created a good definition:

- "Selling the security is still Challenge
- Is the glass half empty or is it half full?
- Security is like the brakes on your car.(Their function is to slow you down, but their purpose is to allow you to go fast)"

In Fig. 1 are presented the Causes of Information Demage created by Prof. Chin - Chu Lo:

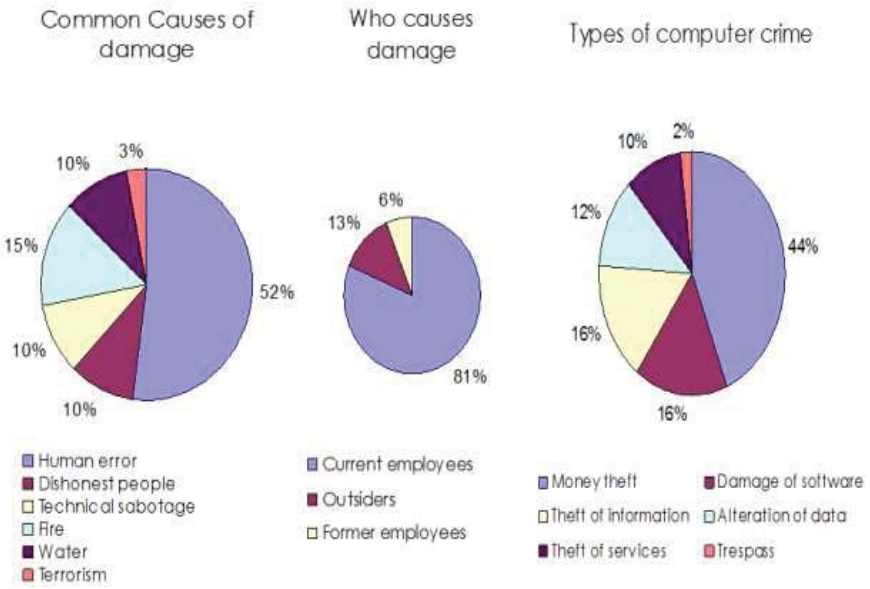

Fig. 1 The Causes of Information Damage (The source: Prof Chi-Chun Lo, National Chia-Tung, University, 2006

5 Advantage of the fiber optic and security issue

Although the information technology is going deeply in nanotechnology, in other side the use of fiber optic is very important field for developing the new medium with high traffic capacity. Before many years is used a conventional fiber optic, but now days are in developing and researching for new fiber optic which can carry more information by following(carrying) multiple light beam. This achievement is potential solution in next generation high speed communications and in carrying biomedical image. This research also impact in developing transmission systems for fiber higher capacity.

The information carrying capacity of conventional optical fibers self is not utilized fully due to the transmission equipments and system limitations. Now we learn about new achievements to increase the information carrying capacity of optical fibers. The new developments in fiber optics will push researchers to develop transmission systems that can tap the hidden potential of optical fibers more. (Today we have 640Gbit /sec or billions bit/sec.). (The electronic devices can operate up to approximately 40Gbps.)

The other way of increase capacity fiber optic is twisted Light Signals which can carry high capacity data in optical fiber.

The market research data by Tele Geography says that the demand for bandwidth grew at a rate of 57% annually between 2007 and 2011.

The optical fiber deployment is growing more than other access technologies

Broadband Forum's report points to a significant surge in ultra-fast broadband, utilizing the data carrying capacity of optical fiber. FTTX (including: FTTH, FTTB, FTTC, FTTP, FTTN etc.)

traditional DSL and hybrid technologies such as VDSL2 contribute to this high growth. These deployment technologies together are supplemented to achieve a 8.6% annual growth.

Last years is developed a transmission and networks through fiber optic as medium for transmission information (voice, data, video, convergence services) for high capacity and nonimpact in electromagnetic field. Although there existing the trust and confidence for this type of transmission through countries in the world, the last of time the doubt begin to introduce through governments in some states or nations. The reason for this is presented in next fragments .

“After hearing the shocking news of sharing individual communication data by internet giants with Federal agencies, now it is the turn of fiber optic cables being tapped by authorities to what they say

'surveillance'. When it is put under the 'National security' and 'Surveillance' people can virtually excuse even private secrets being disclosed in public. Now the reliability of fiber optic networks is under the shadow of doubt. How safe is a fiber optic Network?. Is it totally immune to tapping"? Computerworld, one IT magazine, in April 2003 wrote "Fiber optic cables can be easily intercepted, interpreted and manipulated using any standard off-the-shelf equipment that can be obtained throughout the world. Most important, the vast majority of public fiber networks do not incorporate methods for detecting optical taps, offering an intruder a relatively safe way to conduct corporate espionage." Now they have an article on how to run your own NSA spy program! It was known in 2001, when NSA former technicians revealed that they used special submarine to tap in to undersea fiber optic cables in the mid of 1990s. IEEE reported; "Evidence of the ability of NSA to tap into undersea fiber optic cables and its intention to go on doing it – is a $1B project at Electric Boat in Groton, Connecticut, to outfit a new Navy submarine, the USS Jimmy Carter, with a special 45-meter-long section. The Navy has never disclosed the exact purpose of the expensive addition to the $2.4 billion submarine, but most observers believe it is to tap undersea fiber-optic cables.

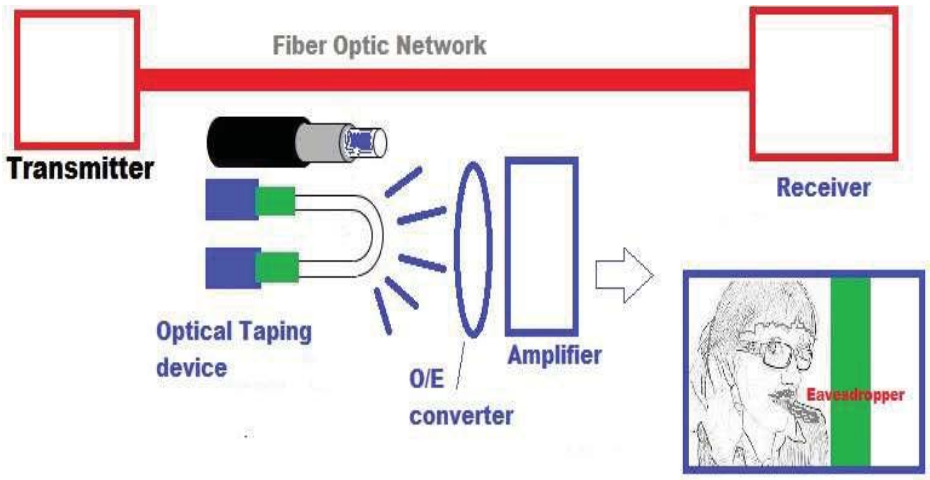

Fig.2. Presentation in the simply mode for Eavesdropping in fiber optic.

"Not only of US or UK, the defense, intelligence, law enforcement, financial and security data of many countries flow through fiber optic cables.
Fiber optic cables are faster and carry huge amounts of data. Fiber optic networks were thought to be safe and secure networks. With the advancement in technology, eavesdropping equipment have also been developed. Ten years before, there was an corporate espionage case on
Verzion's fiber optic networks"
"The conclusion is: fiber optic cables are not exempted from eavesdropping and equipment are available in the market"

Based in those all above I designed the model for business security as in fig.2:

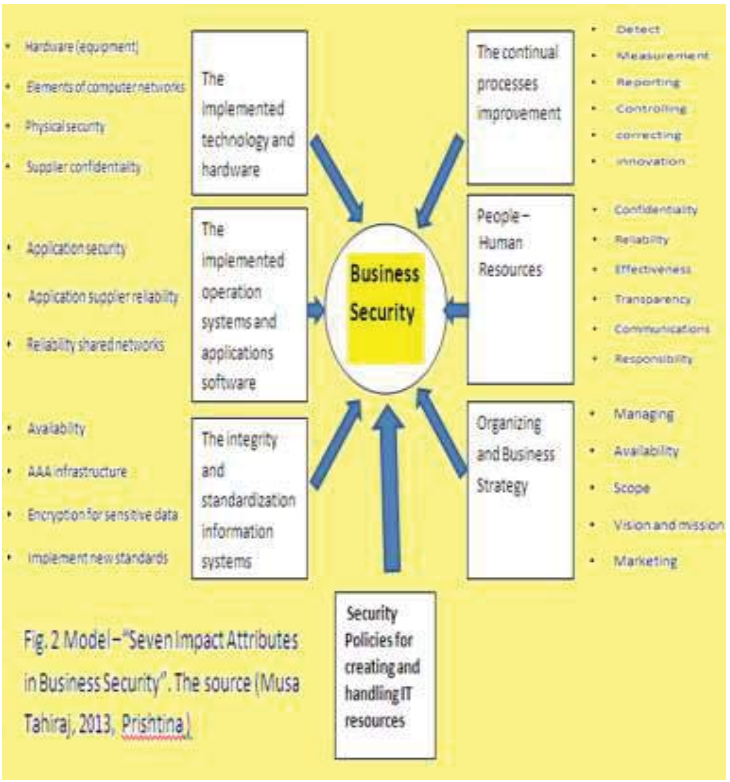

Fig.3. Model "Seven Impact Attributes in Business Security" The source: (The Author)

6 Conclusion and Recommendations

Finding 1: Update and improve continuously security policies and rules for creating and handling the IT resources.
Finding 2: The Human factor (employment) has crucial role in business security informations.
Finding 3: Implement policies in right way by professional staff, and verify for the same implementing.
Finding 4: The information systems are "back bone" for business enterprise progress.
Finding 5: IT Staff must be accomplished with professional knowledge continuously in orders to recovery, create the backups and avoid data damage.
Finding 6: Security is not in high level without coordinating both, professional and the organizational staff.
Finding 7: Investing in secure information systems is profitable issue, ROI will be always in positive side.
Finding 8: The strong enterprise is that have, the stronger and the secure information systems.

References

1. Ralph M.Stair, Georgie W.Reynolds: Fundamentals of Information Systems ,Thomson Couse Technology , Massachusetts, 2008
2. David Anfinson, Ken Quamme: Essentials: PC Hardware and Software Companion Guide, Cisco Press, Indianapolis, 2008.
3. Bruce Schneier: Applied Cryptography, second edition, Jon Willey&Sons, Inc, Mineapolis,1996

4. Allan Reid, J. Lorenz, Ch. Schmidt,: Introducing Routing and Switching in the Enterprise, CCNA Discovery-concepts, Cisco Press, Indianapolis,2008
5. Michael Lee, Gentry Bieker,: Mastering SQL Server 2008,Willey Publishing ,Inc, Indianapolis, 2009.
6. Thomson, Strckland, Gamble: Crafting and Executing Strategy, Mc Graw Hill,New York 2010.
7. Eric Cole: Network Security Bible, Willey Publishing, Inc, Indianapolis 2005
8. Thomas Haigh, *The History of Information Technology*,
9. Annual Review of Information Science and Technology, 2011 ,University of Wisconsin, Milwaukee.
10. Albert Road**,** *How does information security impact you,* Trusted Impact Pty Ltd, South Melbourne.
11. http://www.fiberopticmania.com , *Are Fiber Optic Networks Immune To Eavesdropping* / August/ 2013
12. http://www.osa.org./pressroom release // 02.2009/De-multiplexing to the Max 640Gbit/second.
13. http://www.computerweekly.com/news/ 2240188089/More-than-one-fifth-of-UK-firms-hit-by-DDoS-attacks-in-2012
14. http://pages.arbornetworks.com/TheImportanceof On-PremiseProtection
15. Albert Road, Reducing cost and increasing security, South Melbourne. Trusted Impact Pty Ltd
16. http://www.adt.com/business-security/ September 2013/
17. Berkeley, E.C. Giant Brains or Machines That Think. John Willey &Sons, New York,1949)
18. Tomas Haigh, The History of Information Technology, Annual Review of Information Science and Technology, 2011,University of Wisconsin, Milwaukee.
19. www.telegrafi.com
20. http://www.businesscomputingworld.co.uk/information-security-from-a-business-perspective/#sthash.Q9IeUWAt.dpuf