Содержание:

Introduction

Information technology has changed the business world. As James V. McGee, Laurence Prusak and Philip J. Pyburn (1993, p. 3) point out the way organizations perform their operations, design their products, and market their products have all changed dramatically since the serious introduction of information technology in the mid-1950s.

There are no doubts that the Internet has strongly located in all field of activity of a society in a role of the irreplaceable tool for work with the basic value – the information. Especially in business the Internet is interesting as the tool for communication and information transfer. The Internet gives to firms variety of possibilities: creation of favorable image of a firm or production; increase of availability of the information on firm or production for hundreds millions users of a network the Internet, including geographically removed; cutting-down of costs on advertizing and etc.

According to Kenneth C. Laudon and Jane P. Laudon (2006, p. 9), the Internet and related technologies make it possible to conduct business across firm boundaries almost as efficiently and effectively as it is to conduct within the firm. In other words the companies are not limited by traditional ways to conduct a business. Nowadays the firms maintain close relationships with suppliers, customers and business partners at great physical distances.

At the present time it is very difficult to overestimate the value of the Internet in ability of the companies, the organizations or the enterprises. Every day this service occupies more and more an important place. The Internet becomes the basic business tool, really making profit.

The Internet main task remained the same, as at the time of its origin – accumulation, storage, distribution and an exchange of the diverse information.

Nowadays, there are a lots of managers of the enterprises consider application of information technology as possibility to increase the efficiency of the basic business. It is

reflection of a certain stage of development of the company: the importance of a competition grows, the companies search for additional means of increase of profitability of business. For this reason information technology is some kind of a mode of development and advancement for peak efficiency of activity of the company.

An increased reliance on the Internet is an issue which frequently generates a great deal of heated debate, with supporters maintaining that internet is crucial for the modern business and safe enough, whilst opponents feel that it is internet lead to risk in terms of threats to information systems security. I find myself in the later group. This question is more vital today as ever before, as in the recent years a plenty of different threats and risk using the internet have increased; therefore, it is worth discussing. In this assignment will be considering threats of using the internet and how companies can protect their information systems.

Reliance on the Internet

In recent years there is a rapid development of systems of the telecommunications, one of which key elements is the global computer network the Internet and its main service WWW (World Wide Web). Use the Internet as one of elements of system of marketing can make considerable impact on positive image of firm and on awareness of the consumer about the goods and services. For years of the existence the Internet began to carry out set of various functions. The main function is communication facility possessing the major advantages among which efficiency, reliability, ability to accumulate the information, possibility to supervise communications process, to influence its quality, etc. Another function of the internet is that internet is an integral part of many business processes. It became a place and simultaneously means of interaction of subjects of market relations – commodity producers, sellers and buyers. The most indicative examples of it are electronic commerce (e-Commerce) and the Internet-banking (Internet banking). Speaking about electronic commerce, mean retail trade through the Internet more often. The Internet-banking is a complex of the bank services given in a mode online: informing of the client on a condition of its accounts, remote steering of accounts; payment of utilities, purchase or sale of non-cash currency; crediting, operations with securities, steering of the personal finance, etc.

The Internet has already turned to the original market on which the whole industries work, creating the goods consumed by it and services.

Thus, the Internet became the working tool without which it is already impossible to imagine daily activity of set of people. It and global reference system, and an access mode to technologies, and transport for data transmission, and, at last, an operative and accessible communication medium.

One of the main advantages of Internet technologies is full access to information resources of the company from any point of a global or corporate network. Another aspect that should be mention is that simplicity of use which allows combining the evident form of representation with the simple gear of interrelation of documents. Moreover information systems allow to facilitate steering of the information and to improve communication possibilities.

The main risks and threats to information systems security

Risks of the Internet are connected exclusively from it not by controllability. Being an enormous source of the information, the Internet doesn't divide it on good and bad, or useful and useless.

On the one hand, the Internet provides mass character of its use, and with another – generates a number of problems with serious consequences.

First, the Internet is the port in an external world, it became the basic source of distribution of a harmful mobile code (viruses, Trojan programs).

Secondly, the Internet began to be applied actively as means of the latent penetration into corporate local computer networks.

Thirdly, now the Internet can be considered as one of the basic ports of escape of the confidential information. For example, information resources of the companies are exposed to serious threats because of use by employees of these companies of free mail boxes. Employees of the various companies besides internal corporate mailing addresses actively use the free mail boxes given by various providers (hotmail, mail.yahoo, gmail and etc.). Having access to the Internet from the workplace and knowing that the port isn't supervised, any user can free send any confidential information for organization limits. But even understanding it, not all companies forbid the employees to use free post services. Ports of information leakage from the point of view of prevention of insider

incident are various enough: usb-flash, an instant exchange of messages (ICQ, MSN, etc.), photoaccessories and others.

There are a variety of threats such as computer viruses, worms, spyware and Trojan horses.

Gordon B. Davis and Gordon Bitter Davis (1999, p. 239) point out that a computer virus is a computer program designed to destroy other programs, corrupt stored data, or interfere with the operation of computer system. Computer viruses were and remain one of the most widespread reasons of loss of the information. Despite huge efforts of anti-virus firms competing among themselves, the losses brought by computer viruses, don't fall and reach astronomical sizes in hundred millions dollars annually. These estimations are obviously underestimated, as it becomes known only about a part of similar incidents.

Another kind of threat is Trojan horse. According to Kim Berquist and Anrew Berquist (1996, p. 150) the Trojan horses is an apparently useful program containing hidden code which allows the unauthorized collection, falsification, or destruction of data. The wide circulation of Trojan programs has given to the hacker rather effective tool for reception of the confidential information and destructive activity in relation to users of network Internet.

Programs-spies (Spyware): the software, allowing to assemble data on separately taken user or the organization without their permission. Spyware is applied to a number of the different purposes. The core are marketing probes and target advertizing. In this case the information on a configuration of the computer of the user, the software used by him, visited sites, the statistican of inquiries to search cars and statistics of words entered from the keyboard allows to define a kind of activity and a focus of interest of users very precisely. However the assembled information can be used not only for the advertizing purposes – for example, recieved information about the computer can essentially simplify hacker attack and breaking of the computer of the user. And if the program periodically updates itself through the Internet it does the computer very vulnerable

The deliberate threats-threats connected with malice aforethought of deliberate physical collapse, subsequently system failure. Internal and external attacks concern deliberate threats. The modern history knows weight of examples of deliberate internal threats of the information are tricks of the competing organizations which introduce or hire agents for the subsequent disorganization of the competitor, revenge of employees which are dissatisfied with a salary or the status in firm and other. It is possible to carry threats of hacker attacks to external deliberate threats. If the information system is connected with

a global network the Internet for prevention of hacker attacks it is necessary to use firewall which can be built in the equipment. Hacker attack is an electronic equivalent of breaking of a premise. Hackers constantly crack both separate computers, and large networks. Having got access to system, they steal the confidential data or install harmful programs. They also use the cracked computers for spam sending. The outstanding examples of hacker attacks are attacks Jonathan James. He cracked the serious organizations such as Defense Threat Reduction Agency which is part NASA. After that he has got access to names of users and passwords, and also possibility to look through the confidential information. According to NASA, cost of the stolen software is estimated in 1,7 million dollars. Another example, in the summer of 1995, the Russian hacker by name of Vladimir Levin has cracked electronic protection of Citybank and has stolen 400 000 USA dollars.

There are plenty of natural threats, such as fires, flooding, hurricanes, blows of lightnings. The most frequent among these threats are fires.

Security policy

The lack of security may lead to various consequences and problems, such as loss revenue, lowered market value, legal liability, lowered employee productivity and higher operational costs

Information security is understood as security of the information and an infrastructure supporting it from any casual or ill-intentioned influences which result drawing of a damage of the information, to its owners or a supporting infrastructure can be.

Information security problems are reduced to damage minimization, and also to forecasting and prevention of such influences.

Only the understanding of all spectrum of threats will allow to construct the effective safety system.

It is necessary to give particular attention to e-mail protection as harmful programs often dispatch themselves of nothing to suspecting users.

Necessarily it is necessary to put an antivirus on the corporate server of e-mail. The companies should develop correctly an anti-virus complex in scales of the network, and

than to support its working capacity. Only last versions of anti-virus products are capable to protect users from modern virus threats reliably. To support the protection up to the mark it is required as it is possible to update anti-virus bases is more often. At the enterprise it usually isn't a problem – correctly adjusted anti-virus decision will download and establish updatings in an automatic mode.

The updating of the product is very important. There are new anti-virus modules with each new version, small defects, and at times and errors, in old modules are corrected. That is even more important, in new versions the technologies essentially raising efficiency of struggle against new kinds of cyberinfections are realized. Thus, only last versions of anti-virus products are capable to protect users from modern virus threats reliably.

For information safety, a necessary condition is the equipment of premises in which there are system elements (carriers of figures, servers, archives and etc.), fire-prevention gages, appointment responsible for fire-prevention safety and presence of fire extinguishing means.

Observance of all these rules will allow to reduce to a minimum threat of loss of the information from a fire.

The described modes of maintenance of information security of the company are effective enough to secure the company against set of threats of information security both from the outside, and from within. Though there are also other modes, like total shadowing employees, their efficiency much more low and doesn't get under a category of simple means. Besides, it is not necessary to forget that information security maintenance shouldn't harm to activity of the enterprise or create hindrances for work of employees, after all finally any business processes of the enterprise should be directed on primary activity maintenance, instead of auxiliary services.

The information in the company should be divided into some levels of access. The employee should get access only to those data which are necessary for it for work. The principle of the minimum powers should operate both for electronic, and for other data. It is necessary confirm the list of the most critical information carried to the category confidential, employees should to be acquainted with it under a list. Access to the confidential information is possible only after entering of the employee into the corresponding list confirmed by a management.

Conclusion

Rapid development of information technology has also the negative aspect: it has opened road for new forms of antisocial and criminal activity which were impossible earlier. Computer systems comprise new unique possibilities for fulfillment before unknown offenses, and also for fulfillment of traditional crimes, however, more effective modes.

Threats of safety of information field induce to working out of a complex of the actions directed on drop of risk of occurrence of an emergency situation. For this purpose it is necessary to define first of all set of threats with reference to a concrete segment of information field and an admissible risk level of their realization and to estimate expenses for localization and liquidation of consequences.

The problems connected with increase of safety of information systems, are difficult, multiplane and interconnected. It demands constant, indefatigable attention from the state and a society. Development of information technology induces to the constant appendix of joint efforts on perfection of methods and the means allowing authentically to estimate threat to safety of information sphere and adequately to react to them.

As standard model of safety often result model from three categories:

• Confidentiality – an information condition at which access to it is carried out only by the subjects having on it the right;

• Integrity – avoidance of unapproved version of the information;

• Availability – avoidance of time or constant concealment of the information from the users who have received access rights.

Modern anti-virus technologies allow to reveal almost all already known virus programs through comparison of a code of a suspicious file with the samples stored in anti-virus base. Besides, technologies of modeling of the behavior are developed, allowing to find out again created virus programs. Found out objects can be exposed to treatment, be isolated (to be located in quarantine) or to leave. Protection against viruses can be established on workstations, file and post servers, the gateway screens working under almost any from widespread operating systems, on processors of various types.

From all aforesaid it is possible to draw safely a conclusion that necessity of protection of the information at present costs on the first place. If correctly to choose the anti-virus

software, regularly to update it, and to observe all necessary security measures it is possible to avoid loss, damage of the valuable information and accordingly all consequences.

Bibliography

risk threat confidential damage

LAUDON, K.C., LAUDON, J.P. 2006. Management information systems: managing the digital firm. 9th edn. New Jersey: Pearson Education Ltd.

McGEE, J.V., PRUSAK, L., PYBURN, P. 1993. Managing information strategically. The Ernst & Young information management series.

GGORDON, B. DAVIS, GORDON BITTER DAVIS. The Blackwell encyclopedic dictionary of management information. Oxford: Blackwell Publisher Inc.

BERQUIST, K., BERQUIST, A. 1996. Managing Information highways: the prism book. Dublin: Springer.