Issues of information security in modern business environment

Polina Sergeevna Kolchanova, Jelina Rafajel'evna Torsunova, Anna Grigor'evna Kolchanova

Perm Institute of Economics and Finance, Ekaterininskaja Str., 141, Perm, 614068, Russia

Abstract. The article is devoted to issues of information security of the entity in modern business environment. The authors present the analysis of the information security system on the example of a recording studio, description of security objects, information resources, and systems of forming, distribution and use of information resources of a recording studio. They also analyze measures for protection of information resources of the considered entity and offer actions for information security system enhancement.

[Kolchanova P.S., Torsunova J.R., Kolchanova A.G. **Issues of information security in modern business environment.** *Life Sci J* 2014;11(9s):68-72] (ISSN:1097-8135). http://www.lifesciencesite.com. 12

Keywords: information security, security objects, dangers, information security system enhancement

Introduction

Relevance of a problem of information security is doubtless nowadays. The term “information security” means security of the information environment of the entity from external and internal dangers. Organizational structures of large enterprises provide special departments with the considerable budget which tasks include ensuring information security. Problems of complex safety of large organizations and the entities are described in scientific works. Issues of information security regarding different countries are considered by C. J. Bennett. [1]

Material and Research Methodology

Issues of personal security are described by L. Floridi [2]. Issues of information security in mobile services are considered by Orman, H. [3], Raj, A., Suryanarayanan, R., Claudatos, C. H., Basavaraj, S., Fernandes, J. E., Sheshadrivasan, S. M., & Visweswaraiah, D. [4].

Issues of information security are described by D. Desimone, M. H. Reider, K. Geist & V. Gonzalez [5].

Issues in the field of storage of informative data are considered by Graves, T. M., McLeod, A. C., & Tynan, P. [6].

Issues in the field of the fundamental principles are described by Hosein, G. [7].

Unlike large enterprises, information security of small enterprises with a small number of workplaces is not streamlined. However, currently the majority of existing dangers of information security become challenging for the entities of the smaller size due to the fact that large entities are well-protected. It often happens that such entities have rather small IT-budget, allowing to purchase only the necessary equipment, the software and to hire one system administrator [8].

For this reason the problem of development of action plan for enhancement of an information security system at small enterprises by means of hardware and software arises.

The research goal is enhancement of an information security system at small enterprises on the example of "KR" recording studio.

Research objectives: analysis of security objects, analysis of an operating information security system of the recording studio, reveling of dangers of information security, reveling of weak spots of information security, development of actions for removing weak spots of information security.

Following methods were used in research process: theoretical research methods such as analysis, comparison, generalization; empirical research methods: interview, observation, inspection; general scientific methods: comparative method and method of the system analysis [9].

The research object is "KR" recording studio, which owns a lot of information resources, including the intellectual property, which is protected with software and technical means of information security [10].

Results and discussion

"KR" recording studio’s security objects include: information resources (trade secret, confidential information, open information) [11]; the system of forming, distribution and use of information resources (information technologies, procedures of collection, processing, storage and information transfer, users and service personnel); information infrastructure (center of information (data) processing and analysis, hardware and software of its processing, transfer and display, including the channels of information exchange and communication, location where processing of documentary information with limited access is carried out and negotiations of confidential character are held) [12].

Information resources of recording studio are stored in electronic form on the server, at workstations of the studio's personnel and removable hard drives. Information resources on papers are stored in designated areas: offices of the sound producer and the head of the studio.

Users of information resources are: clients and other partners of the recording studio; tax authorities; personnel of the recording studio.

Special department on the information maintenance and protection is absent. The system administrator is reliable for the protected information. Following ways of the information transfer depending on its properties and aim of distribution are popular at the enterprise: transfer of preliminary version of the product to the client by means of the mail agent, use of the removable media for transfer of the ready product to the client, transfer of materials for work by means of a local computer network.

Procedures of use, storage and processing of information resources are performed by means of the following software: ACID music studio 8.0, Sound Forge Pro 10.0, Melodyne Editor, Cubase 5, MixMeister Fusion, YoGen Vocal Remover, Studio One 2, CD architect 5.2, Time factory, Wave Lab 6.

The topology of a local computer network has star-shaped structure consisted of four personal computers and the server set on the virtual machine of one of workstations. The cable network is connected by means of a hub. Signals from the transferring computer arrive via the hub to all other computers. Each computer of a network has the personal IP address in one subnet. The server is situated on the virtual machine on which the Windows Server 2003 operating system is installed.

Following models of the equipment are used at the recording studio:

✓ AMD Athlon™ II X2 Dual-Core base unit;

✓ Samsung 220TN liquid-crystal monitor;

✓ Canon PIXMA iP4940 inkjet printer.

Security objects of the recording studio can be subject to the following dangers [13]:

Personnel of the enterprise can purposely or accidentally cause distribution of confidential information, for example by e-mail, ICQ and on other digital means of communication that can affect reputation of the studio due to personnel access to the recording studio's data.

Unauthorized use of the commercial information for leaking it to competitors of the recording studio. It can affect the studio's activity, in particular client basis, reputation in show business, and also financial position at large.

Theft of intellectual property through a network or physical theft of media (a removable USB device, a removable hard drive with confidential information).

Unfair duty performance by personnel of the recording studio, in particular inadvertent distortion, deleting a musical material, can lead to conflict situations with the recording studio management, and also with clients of the studio.

Failures of the recording studio's software and hardware due to the fact that any equipment can glitch in use. This danger can break a schedule of operations that can lead to loss of trusting relationships with clients, and also to violation of a schedule of personnel operations.

Failure of supporting infrastructure: violation of operation of a heat supply, conditioning, power cutoff, - all these factors can cause infringement of information resources integrity, and also stop the recording studio' activity for an indefinite term that will affect a financial status of the studio.

Computer viruses infiltration to the recording studio's system via removable media of information, a computer network, and the Internet network can lead to distortion of confidential information, work files, and also to loss of data. It will take a lot of time to recover the system and the damaged data that will lead to violation of a schedule of work.

Storage of confidential information on papers can lead to unauthorized reading, change, and also to information destruction.

Information security of the recording studio is performed in a complex and includes the following actions:

2. To protect the information from the danger of unauthorized use of the commercial information for leaking it to competitors following actions performed: distribution of access to computers at the level of the administrator (system administrator) and at the level of the user; setup of accounting entries and the login organization by means of built-in Windows means; application of an installed system of remote control.

3. To protect the information from theft of information resources by means of removable media following actions performed: alarming system set in the studio, and a running contract signed with non-departmental security forces for location protection; limited access to personal computers of the studio's personnel and to the corporate server; treillages installed on the windows.

4. To protect the information from inadvertent distortion of musical material personnel back up the information after completing the operation on the PC.

Data necessary for the employees is situated on the corporate server in the network-attached storage.

5. To protect the information from failures of the recording studio's software and hardware following actions performed: actions for creation of the system's restore point in case of a failure; planned inspections of operability and maintenance of all information systems and information infrastructure; backups due to the mistakenly damaged file or system, in case of serious accidents or in need of files recovery over the past periods of time.

6. To protect the information from failure of supporting infrastructure the studio uses an uninterruptible power supply unit, capable to provide a power supply for the local computer network.

7. To protect the information from computer viruses infiltration to the recording studio’s system following measures taken:

1) special utilities which monitor network condition and alarm in case of detection of certain events, concerning information security of the recording studio;

2) in the field of access to the special software on the server : router and firewall. The data interchange with the Internet network is performed only according to protocols which are really used in the recording studio (http, tcp/ip). Data interchange attempt according to unauthorized protocols is locked with a firewall and registered in logs. Exchange of NETBIOS packets with the Internet is forbidden. Local firewall with network access settings for certain applications is set on users' PCs. Settings of local firewall are password-protected.

3) the license anti-virus program (Dr.WEB) which is continuously checking all loaded files from the Internet. Up-dating of the software product is made on the corporate server by the system administrator of the recording studio.

Following weak spots were revealed during analysis of the existing information security system of the recording studio:

Personnel have insufficient knowledge rules for protection of confidential information; they do not realize the need of their careful performance. It is expressed in purposeful or accidental cause disclosure of confidential information and distortion of musical materials.

Insufficient security of intellectual property connected to the danger of theft of necessary information by interested persons through the Internet network.

Storage of confidential information on papers on personnel's tables that allows malefactors to use it easily.

To remove weak spots, revealed in the studio’s information security system, the authors offer to take following actions:

1. Recommendations about the equipment of locations.

2. The design of locations should exclude possibility of visual viewing of processed or transferred information by other persons (visitors or other employees).

3. Location should be equipped with strong input doors with safe locks to ensure safety in non-working hours.

4. Location should be equipped with security and fire alarms and after the end of a working day shall be sealed and passed for secure keeping.

5. Recommendations about protection against illegal access.

6. All workstations of the recording studio should be equipped with security features against illegal access (SF IA).

7. Each employee of the recording studio should have the personal touch memory identification number (TM ID number).

8. The system administrator of the recording studio should control operation of SF IA and distribute TM ID numbers.

9. Recommendations about password protection.

10. Password protection in automated systems prevents any accidental or deliberate actions which lead to unauthorized acquaintance with the confidential information, its distortion or destruction, or make such information unavailable to authorized users.

11. Password protection assumes personal identification of the user and the processes initiated by this user, ID authentication of the user (password entry), registration (recording) of operations of mechanisms that control access to resources of the automated system with specifying of a date and time, required resources, results of performance, including the forbidden access attempts.

12. Personal passwords are selected by WKS users independently, but taking into account the following requirements: password length – at least 8 characters; there should be letters of upper and lower rails, digits and special characters (@! &, *, %, etc.); the password should not include easily calculated combinations of characters (names, surnames, names of WKS, etc.), and also the standard abbreviations (PC, LAN, USER, SYSOP, etc.); in case of password

change new password should differ from the previous one at least in 6 symbols; change of passwords in the process of operation should be made timely.

13. The system administrator of the recording studio should control activities of employees to ensure password protection of information resources.

14. Recommendations about virus protection.

15. Means of virus protection of information should be applied on all WKSs.

16. Procedure of installation and the regular up-dating of the virus protection software (versions of the software and bases of viruses' descriptions) on every WKS should be organized in an automatic mode and be controlled by the system administrator.

17. It is necessary to organize anti-virus filtering of all electronic exchange traffic and all information arriving via removable media.

18. The system administrator of the recording studio should control operation the virus protection software.

19. To eliminate the danger of theft of information resources through a network the authors offer to use stream filtering of Internet-traffic of the recording studio's personnel (the certified version of eSafe software) and, if necessary, to block Internet-traffic to prevent transmission of confidential data.

20. To eliminate the danger of disclosure of confidential information by the studio's personnel authors offer to hold a number of consultations about information security for employees to understand the importance and confidentiality of the information entrusted to them. Usually, the reason of disclosure of confidential information is insufficient knowledge of rules for commercial secrets protection and unawareness (or misunderstanding) of need of their careful keeping.

21. In case of distortion of information resources by the recording studio's personnel, management is offered to give a warning or admonition with following premiums deprivation depending on the degree of information distortion. In case of violation of the recording studio's activity and work process because of information distortion by the employee, management is offered to dismiss the employee with the appropriate recommendation letter.

22. To eliminate the danger of unauthorized access of the information on papers it is offered to minimize the number of transferred paper documents in the recording studio and to transform necessary documents into the electronic form to increase the level of security.

Electronic documents should be stored on the corporate server and on the personnel's WKSs according to performing tasks.

The offered actions for improving the information security of the recording studio will allow:

- to enhance the level of reliability of the information security system;
- to reduce the risk of loss and unauthorized change of information;
- to enhance the level of WKS security;
- to enhance the level of personnel's responsibility for the actions;
- to regulate the enterprise's activity at large.

Despite the huge list of the information security features, none of them can guarantee absolute reliability and safety of information resources, but the offered measures with the integrated approach to issues of the information security can minimize possible risks.

Conclusion

Summarizing the results of this research the authors came to the following conclusions.

In the course of this research the authors analysed the security objects, operating system and information security features of "KR" recording studio, dangers for information security, and also revealed some weak spots. According to the revealed weak spots they offered actions for their elimination.

The human factor, circumstances of insuperable force, and also prompt development of information technologies (the virus software) will always take place.

If protective measures will not be taken, expenses for the information recovery and the lost opportunities will exceed the cost of security system development.

Corresponding Author:
Dr.Kolchanova Polina Sergeevna
Perm Institute of Economics and Finance
Ekaterininskaja Str., 141, Perm, 614068, Russia

References

1. Bennett, C. J., 1992. Regulating privacy: data protection and public policy in Europe and the United States. Cornell University Press.
2. Floridi, L., 2014. Open Data, Data Protection, and Group Privacy. Philosophy & Technology, 27(1), pp: 1-3.
3. Orman, H., 2013. Did You Want Privacy With That?: Personal Data Protection in Mobile

Devices. Internet Computing, IEEE, 17(3): 83-86.

4. Raj, A., R. Suryanarayanan, C.H. Claudatos, S. Basavaraj, J.E. Fernandes, S.M. Sheshadrivasan, and D. Visweswaraiah, 2014. U.S. Patent No. 8,655,966. Washington, DC: U.S. Patent and Trademark Office.
5. Desimone, D., Reider, M. H., Geist, K., & Gonzalez, V. 2013. U.S. Patent No. 8,386,705. Washington, DC: U.S. Patent and Trademark Office.
6. Graves, T. M., McLeod, A. C., & Tynan, P. 2013. U.S. Patent No. 8,504,787. Washington, DC: U.S. Patent and Trademark Office.
7. Hosein, G., 2013. Returning to a Principled Basis for Data Protection. Chicago-Kent Law Review, 84(3), pp: 7.
8. Degtyarev, V. V. Ensuring information security of small enterprise with simple means. Date Views 01.03.2014 www.ab-solutions.ru/.
9. Portal of young scientists. Date Views 01.03. 2014 www.dissertant.uz/view_post.php/.
10. Site of recording studio "Kanta Records". Date Views 01.03.2014 www.kantafm.ru/.
11. The federal law of the Russian Federation "About information, information technologies and about information security" of 27.07.2006 #149.
12. Trubilina, I.T. (Ed.) 2000. The automated information technologies in economy. Moscow, Finance and statistics. pp: 416.
13. Galatenko, V.A., 2004. Bases of information security. Internet university of Information technologies INTUIT.ru. pp: 280.

5/27/2014