ANNALS of the ORADEA UNIVERSITY.

Fascicle of Management and Technological Engineering, Volume VII (XVII), 2008

STUDY REGARDING DATA SECURITY AND SAFETY IN SMALL AND MEDIUM-SIZED COMPANIES

Naiana ȚARCĂ, Ioan ȚARCĂ
University of Oradea
e-mail: ntarca@uoradea.ro, nelut@uoradea.ro

Keywords: data security, data safety, backup, data lose, working discipline

Abstract: This paper presents the results of a study regarding data security and safety issues in small and medium-sized companies. The study regarded the employees from different functional compartments/departments, excluding the informatics department. This means the employees with no special skills in informatics, but with minimum computer operating knowledge. The scope of the study was to find the measure in which the employees are awake to the importance of their working data security and safety issues.

1. INTRODUCTION

This paper presents the results of a study regarding data security and safety issues in small and medium-sized companies.

Data security and safety issues are increasing together with the company's degree of activity's automatic data process. The connectivity and information access emphasis generates new data security problems.

Data security and safety issues depend not only on technology and processes used but also on people. For this reason we approached data security and safety from the employees' point of view.

The study regarded the employees from different functional compartments/departments, excluding the informatics department. This means the employees with no special skills in informatics, but with minimum computer operating knowledge, because current working file saving and maintenance (word, excel, power point, access, etc) are their responsibility.

The scope of the study was to find the measure in which the employees are awake to the importance of their working data security and safety issues.

2. THE EMPLOYEES' ROLE IN INFORMATION SECURITY AND SAFETY ASSURANCE

Usually, employees have to obey rules regarding workstations' and software use, and those regarding information securities. Thus, each employee has to:

- save their current files at the end of the working day, to close all the applications and safely shut down the computer
- keep secrecy on the system access passwords these being private and for their own use; each password is associated with specific politics and rights which grant access to specific data, which could be abused by someone who enters the password possess
- use hard to decrypt passwords
- not to leave passwords on desk-forgotten jotters
- close the applications each time they leave the workstation
- logout whenever they leave their workplace for a prolonged period of time
- lock the station using password in case they leave the working place for short-time

- destroy all documents on paper support created through application software which does not make the object for archiving
- create backup copies on different media for working data and documents
- use the Internet only for professional purposes to facilitate access to interesting information for their activity, for Microsoft software activation and software up-to-dates: antivirus programs, Microsoft products and operating systems update
- to keep secure the Internet access account and password because unauthorized use may result in abuses or Internet misuse
- not to configure Internet access on unsecured workstations, without antivirus or firewall applications correctly configured or to use unsecure browsers
- not to install virus-susceptible programs to avoid problems concerning workstations or network security and stability
- not to subtract data, documents or information generated with software applications which can bring prejudices to their company
- not to use external memories (diskettes, CDs, flash memory) without prior control made by the informatics department to avoid virus or malware contamination.

In order to obey these rules, the employees need to know them and take them seriously. That is why the employees education is important together with the presentation of the consequences that occur in the case of disobey. When people understand the role they play in information security, they become more collaborative.

Perhaps the most efficient and cheap anticipation measure for a company in securing its data is to achieve the employees support for this activity.

3. DATA ANALYSIS AND INTERPRETATION

Three hundred questionnaires were sent through e-mail and 200 by ordinary mail to collect data to arbitrary chosen small and medium-size companies. Among them 261 were returned and use for data analysis thus resulting a response rate of 52,2%.

The questions were grouped as follows:

1. Questions regarding the employees' age and degree level.
   Regarding the age, following groups were established:
   - Between 20 and 30 years
   - Between 30 and 40 years
   - Between 40 and 50 years
   - Over 50 years

   Regarding degree level, the categories were:
   - High school
   - Superior studies
   - Master degree
2. Questions regarding the aim of computer use (document creation, data base management, internet browsing, internet communication)
3. Questions regarding the way in which employees regard the possibility of losing or stealing data.
4. Questions regarding the measures that employees use to secure data and to avoid their lose

Among responding persons 92 were between 20 and 30 years, 68 were between 30 an 40 years, 59 were between 40 and 50 years and 42 were over 50 years.

Collected data showed that:

- employees between 20 and 40 years of age pay a greater attention to data security and safety than those having over 40 years
- employees over 50 years are the most unaware on the fact that they can lose important data and documents created in a long period of time or the fact that other employees could access confidential data due to their negligence

Results are synthesized in the table below:

Data security and safety assurance / Age group (years)	N	A	B	C	D
20 – 30		8	87	92	9
	%	8,69	94,56	100	9,78
30 - 40		7	61	68	8
	%	10,29	89,7	100	11,76
40 – 50		9	48	52	3
	%	15,25	81,35	88,13	5,08
> 50		12	26	35	4
	%	28,57	61,9	83,33	9,52

A - have communicated the system access password to other persons, allowing thus confidential data access

B - block the workstation using password when leaving it for a short period of time

C - create backup copies of the files for recovering purposes

D - external memory media on which data are being backup are used to backup data on their personal PCs at home

Among the persons that returned the questionnaires 82 graduated the high school, 124 graduated a faculty and 55 graduated a master.

Collected data showed that:

- the higher the graduated level the greater the importance of data security and safety is considered.

Results are synthesized in the table below:

Data security and safety assurance / Graduated level	N	A	B	C	D
highschool	%	32 39,02	51 62,19	71 86,58	18 21,95
universitary studies	%	3 2,41	118 95,16	121 97,58	4 3,22
master degree	%	1 1,81	53 96,36	55 100	2 3,63

4. CONCLUSIONS

On workstations at the workplaces are placed information which generally demand a great working volume. Their lose or access by unauthorized people depends in a great measure on the way in which the employees treat data security and safety issues.

In the case of backup copies lack, the user need to recreate its documents in case of unwanted events, starting practically from the beginning.

To avoid data lose or unauthorized access in destructive purposes, an important role is played by the working discipline: Avoidance of password communication to other people, thus preventing them to access the system, the avoidance of virus spreading through the use of unchecked external media, also used in other places/purposes, installation only of the licensed programs, avoidance of unknown mail opening.

The aim of the study was to reveal the influence of the graduated degree and the age on the way in which employee action toward their information security and safeness.

It has been noticed that information security and safeness assurance inside a company depend in a greater measure on the employees' graduate degree that on their age.

BIBLIOGRAPHY

[1] Oprea D., Protecția şi securitatea informațiilor, Ed. Polirom, 2007
[2] Thomas T., Primii paşi în securitatea rețelelor, Ed. Corint, 2004
[3] Zisu C., Mihalcea A., Securitatea sistemelor informațional–decizionale, Ed. Tritonic, 2007
[4] Whitman M., Hands–on Information Security, Thomson, 2005
[5] Whitman M., Mattord H., Principles of Information Security, Thomson, third Edition, 2007
[6] Whitman M., Mattord H., Management Of Information Security, Thomson, 2/E, 2007
[7] www.east-tec.com
[8] www.informit.com
[9] www.pcprivacycentral.com