CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

Department of Information Technologies

Comparison of data security in different types of firms

Diploma Thesis

Author: Bc. Tereza Součková

Supervisor: RNDr. Dagmar Brechlerová, Ph.D.

Czech University of Life Sciences Prague | Faculty of Economics and Management

Department of Information Technologies

Academic year 2008/2009

DIPLOMA THESIS ASSIGNMENT

Tereza Součková

specialization of the study: Informatics

In accordance with the Study and Examination Regulations of the Czech University of Life Sciences Prague, Article 17, the Head of the Department assigns the following diploma thesis to

Thesis title: **Comparison of data security in different type of firms**

The structure of the diploma thesis:

1. Introduction
2. Objectives of thesis and methodology
3. Literature search
4. Analyse of data security
5. Comparison of firms
6. Conclusions
7. Bibliography
8. Supplements

The proposed extent of the thesis: 50 - 60 pages

Bibliography:

[1] SALOMON, David. Data Privacy and Security. 1 edition. Springer, 2003. ISBN-10: 0387003118.

[2] PFLEEGER, CH., PFLEEGER, S. L. Security in computing. Prentice Hall, 1997, 2003. ISBN 0-13-035548-8

[3] BISHOP, M. Computer Security. Art and Science, 2005. ISBN 0-201-44099-7.

[4] GOLLMANN, D. Computer Security. 1999. ISBN 0-471-97844-2

[5] MENEZES, A. J., VAN OORSCHOT, P.C. A VANSTONE, S.A. Handbook of Applied Cryptography. CRC Press, 2001. ISBN 978-0849385230

The Diploma Thesis Supervisor: **RNDr. Dagmar Brechlerová, Ph.D.**

Deadline of the diploma thesis submission: April 2010

.....
Head of the Department

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE
Provozně ekonomická fakulta

.....
Dean

In Prague: 22th December 2008

Declaration

I declare I have produced my Diploma Thesis with the title **Comparison of data security in different types of firms** on my own using the professional literature and the expert consultation with RNDr. Dagmar Brechlerová, Ph.D.

In Prague:

.....……..

Tereza Součková

Acknowledgement

I would like to thank Mrs. RNDr. Dagmar Brechlerová, Ph.D. for all the beneficial advice, Mr. Pavel, Mr. Hána and Mr. Michálek for all the advice and all the information they were willing to give to me. I also have to thank my family for their support during my study.

Comparison of data security in different types of firms

Zabezpečení dat ve firmách různého typu

Summary

The objective of this Diploma Thesis is to gather suitable material in a form of a literary recherche, which will be used in the analysis of data security in the system of a company, and to make a comparison of the security level of these companies. Observed companies differ in the number of their employees and in their field of activity. These aspects could be a reason to suppose that the measure and the way of data security system are different as well.

Key words

Data security, personal security, computer threats, virus, worms, security features, backup, archiving, data recovery, safety audit

Souhrn

Cílem této diplomové práce je shromáždit vhodný materiál v literární rešerši, který bude využit při analýze zabezpečení dat v systému firmy, a provést srovnání úrovně zabezpečení těchto firem. Pozorované firmy se liší počtem zaměstnanců a oborem činnosti. To může být důvod se domnívat, že míra a způsob zabezpečení je také rozdílný.

Klíčová slova

Datové zabezpečení, personální bezpečnost, počítačové hrozby, viry, červy, bezpečnostní prostředky, zálohování, archivace, obnova dat, bezpečnostní audit

Content

1 Introduction

Nowadays everyone of us has some kind of information which is needed to be stored somewhere by using data media. People want to use and work with some information. They use information systems and many applications. Data present a main part of the information systems. Data are sent and received. Data are shared and there is a data access. If person wants to use data and work with them, he needs to adhere to some rules. It depends on how data are used and how much sensitive the data are.

There are basic approaches how to save data and how to prevent from misuses. This is mainly solved by the information security. In case the possible kinds of dangers and threats are known, it is easier to defend against it. If people care about the security and they are still on the lookout, the risk of misuses, loss or damage is lower.

In case the information system is a part of the company which works with the data and these data are source of the company profit, it is necessary for the data to be protected, shared and become available only for competent users. If attention to data security is paid from the beginning with a higher probability there will be no causes of a financial loss or even an advantage of competitive companies.

The development and importance of information systems and new technologies grow up in the world. So it is obvious to care about new possible dangers and threats against data security. The Internet is used for searching for information, for purchasing and selling of goods, for internet banking, sending and receiving e-mails and so on. It is evident that for every operation some kind of data is retrieved or provided. If data are sensitive, data security has to be assured. Unfortunately, there is no existing system which is totally secure.

The companies which are present part of the research of this diploma thesis use many kinds of data and treat it. Every manipulation with the data must be performed with a precaution. If there is a data operation which is illegal or which causes damage, a sanction or a resolution have to follow. The solution how to avoid an accident is to be aware of every possible threat and to build a system which is resistant to these threats. Every company has possible threats. Some threats are common, some threats are

specific. It depends on a field of activity of these companies. There are also different solutions depending on responsible employees as well as on the company budget spent in order to make a highly protected system.

An analysis of every company is performed in order to find out if these companies are able to protect their data and adhere to rules. There is presented a comparison of the different data security of the different companies.

2 Objectives of the thesis and methodology

2.1 Thesis objectives

One of the objectives of this Diploma Thesis is an analysis of data security in three existing companies and a comparison of these companies. The comparison should reveal differences or similarities of data security of these companies which work in a different field of activity, employ a different number of employees and process different quantity of data. All these reasons should cause a different degree of data security.

2.2 Methodology

The analysis of the companies is performed in a form of a literature recherche. Each part of data security analysis is examined step by step. In order to obtain corresponding information an interview with a data security specialist or a responsible employee was made. Employees answered the questions in a form of a questionnaire related to the password security. Methods for quantifying these results, called Scoring method and SWOT analysis, are used to analyse the results of the research and to compare these results.

3 Literature search

3.1 Data significance

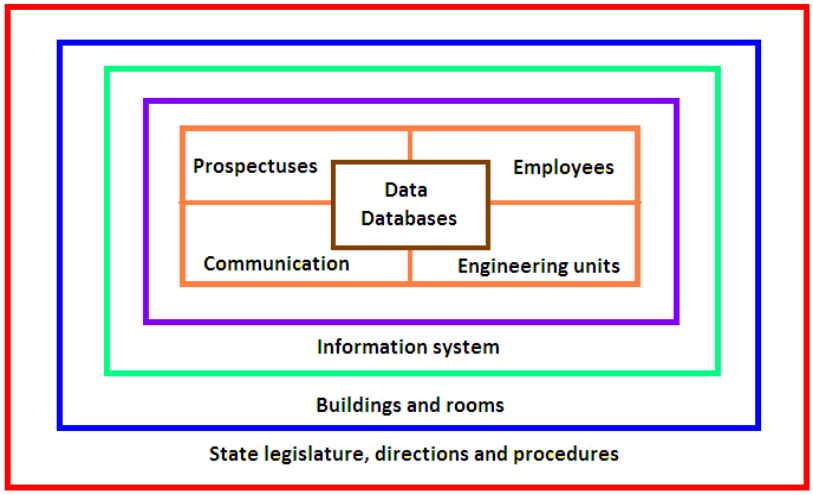
The data significance is obvious. It is a need for everyone to store their data. Nowadays it is possible to use many different devices for data sharing. There are magnetic media, optic media or electronic media. When there are some data to be stored, it is necessary to think about their protection. It really depends on where the data are stored, who can share them, and so on. It is necessary to think about possible threats and what is a possible defence. This is a way how to ward off a data loss and an abuse of data of a different kind of importance. [1]

3.1.1 Secure information system

A security of an information system means a security of the information during its creation, savings, transmission, manipulation and liquidation. There are certain measures used during these operations: logical measures, physical measures, technical measures and organizational measures. All these measures should counteract a loss of confidentiality and have to vindicate for an availability of all these levels of measures.

An information system is composed of few parts. Hence an information system has to be built as a complex of protection mechanism applications and then it could be considered as a safe information system. [1]

Fig. 1: General model of an information system and its environment



Source: DOBDA, Luboš. Ochrana dat v informačních systémech.

3.1.2 Physical security

There are buildings and rooms, where the system is stored physically. The security goal is to protect this environment. There could occur an inadvertent access of strangers which means there has to be ensured an object security as a protection against a theft. Monitoring system, system of barriers and control of movement of persons with identification cards should be presented as well. The media have to be stored safely and destroyed safely as well. The server room as the core of many business information has to be secure properly. The physical security also means system has to be protected against the natural influences such as weather conditions, floods, fires. It also includes ensuring a continued stable supply of electricity. [1]

3.1.3 Personal security

Personal security means a protection against the human element. There are employees in an information system and so the protection of employees has to be ensured, but on the other hand the protection against an unpermitted manipulation of employees has to be ensured as well.

It is good to know that there are different kinds of personal threats. There is an unauthorized alteration of access privileges for employee or rights for other employees, a premeditated or unmeant data corruption. There are changes of an information system configuration, refusal of a safety code, illegal installations of software and its usage.

It is necessary to be informed about a life cycle of the staff. It is divided into four stages: selection of a new staff member according to the required criteria, training phase, management and continuous improvement of the staff member and termination of the employment and followed by leaving the workplace. Each stage involves certain risks, but the last stage involves the maximum risk. An employee carries away some information that could be confidential.

When there occurs a termination of an employment, the employee has to be instructed about obligations arising from contract. Mainly the employee should be bound to secrecy in writing (signed secrecy agreement). [1]

3.1.4 Mode security

Mode security presents a complex system of administrative measures and control components. Security has to be ensured because each information system is part of the environment. It is related to the international agreements, laws, regulations and social norms.

Defined procedures, means of an action and methods are to be followed for a safe operation of an information system. It means a procedure to log on and log off, methods for testing required security parameters, methods for marking and recording media and procedures for their destruction, the use of a cryptographic protection and others. [1]

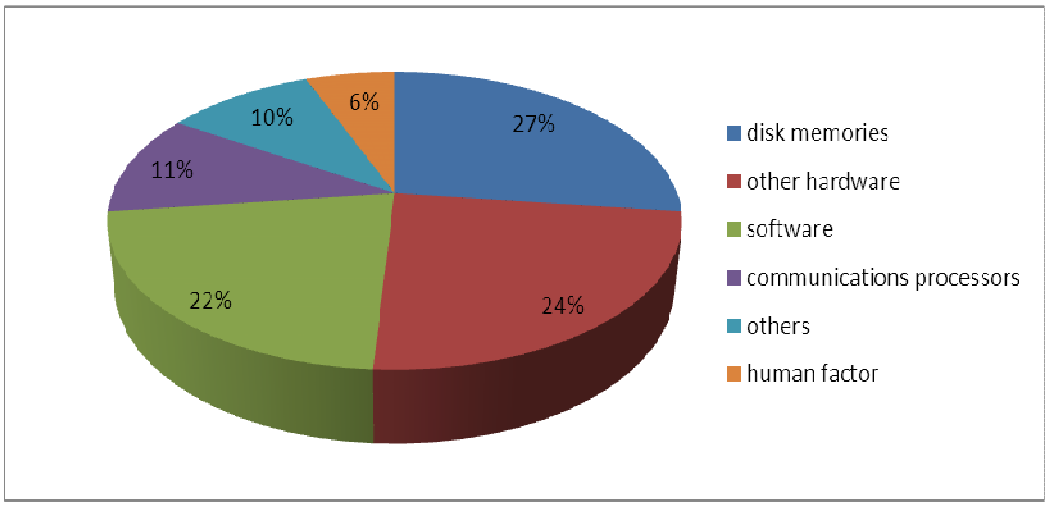
3.1.5 Technical security

None of technical elements work without errors. It is suitable to make a high-quality selection and an assurance of a sufficient safety and services.

The basic problem of a relation between technical equipment and data is a disk memory. These devices contain components which are slow and faulty. Disk operations

represent 50% of a computer performance but as it results from the graph they represent also 27% of total sum of failures. [1]

Fig. 2: Frequency of individual types of errors due to computer



Source: DOBDA, Luboš. Ochrana dat v informačních systémech.

3.1.6 Software security

Software security means the security of all of the software equipment, which consists of the operating system, the system for application and database operations, the compliance with licence conditions and the check-up of access to programs. The security increases when there is a best selection of security qualities and operating reliability. When reliable programs and various methods are used such as restricting the programming resources, allotting data and a storage space and various security models, it represents the protection of the integrity, access control and more. [1]

3.1.7 Data security

It is necessary to protect the data within files and databases against an unauthorized modification, damage, loss or a theft. It is suitable to use an antivirus protection and an access check-up for the data. Requirements for data security are mainly based on data integrity, auditability and availability. [1]

3.1.8 Communication security

Communication security means a protection of communication paths, confidentiality and integrity of all the information between different parts in the structure of the LAN - local area network - inside and outside the structure which is represented by the WAN – wide area network. The computer is the most secure, if this machine is not open for surroundings. The source of a danger for network computers can be sharing facilities, the technological complexity, the high number of potential vulnerabilities and various network attacks in various places in the system. [1]

3.2 Threats against data security

There are few categories of possible threats. The probability of an accident is lower if we know these threats and we can secure our data against them. The human factor is mainly responsible for the accident; he is also a main creator of malware. Malware is every application causing any type of data damages. There could be an employee using an irregular way of a data manipulation. There could be an unexpected accident related to technical problems or natural hazards.

3.2.1 Malware

A mmalicious software, shortly called Malware, is divided into several groups. We can distinguish malware according to the location in a memory - Resident and Non-resident type. We can distinguish malware according to the affected areas – Boot, File, Extension, Overwriting, Duplicating, Cluster, Macro viruses and Retroviruses. We can distinguish malware according to the behaviour and the detection - Stealth and Substealth, Polymorphic, Slow and fast infector, Armour and Sparse. [10]

Fig. 3: The scheme of most abundant types of malware.

Source: http://www.anyplace-control.com/blog/media/blogs/index/malware.jpg [cit. 2010-12-28].

3.2.1.1 Viruses

Virus is a piece of a programming code that can be replicated through the host application, not just once. And nowadays, there is a slight difference between a virus and a worm. Especially it is related to electronic e-mails.

Viruses are spread in several ways. CDs, DVDs, flash discs, e-mails, files from the Internet and other possible media are used.

It is possible to notice specific viral symptoms. The most common indicator is a situation when the implementation of programs takes longer than before. Another situation could be when some files disappear and new files appear. The disc is more active than before. Free hard disk capacity is reduced and some names of files are changed without any explanation. The hard disc is inaccessible.

The consequences of a virus infection have different forms. It could be a harmless visual and sound effects that distract the user and reduce a computer memory. There could be a possibility of destroying data and programs.

The total number of viruses is not known, but the approximate number was around 100 000 viruses in 2004. [5]

3.2.1.2 Worms

The worm is very similar to a virus, but the worm is able to produce clones of itself. In some cases the worm is modified to become uneasily detected by the security software. The worm takes control over the network communication services in order to subsequent spread to other places.

The main tasks of the worm is the complete system stall or a part of system, deleting files stored on the disc, getting sensitive data in order to make a profit, an abnormal behaviour of the operating system and etc.

The most dangerous worm of last few years has been Win32/Conficker. This worm has been spread through the Internet and it has exploited the vulnerability of network services for sharing directories in the Windows operating system. [5]

3.2.1.3 Trojans

Trojan is a type of a virus code hidden in the file, which could be executable or not. Trojan is hidden from detection programs. Trojan starts after passing safely checking. The infected file could be considered harmless. Trojan could be represented by any archival program, any game, or even an anti-virus program.

The most common types are password-stealing Trojans and a backdoor.

Password-stealing Trojans are in a group of Trojans, which monitor every push of the keyboard and information is saved and send to Trojan creator's e-mail. They acquire information and use them to make a profit.

The backdoor is a client/server application. It acts anonymously; the user has no possibility to observe it. This application is used for a remote computer management and it may not be harmful. It depends on activities of users which carry out this management. It is also related to the way of installing the worm in the system.

Another type is a classical form of Trojan horse, which destroys files on the disc or the disc is completely formatted. Usually the file with bin .BAT is detected as a Trojan. [5]

3.2.1.4 Adware

Adware is used as a view of an advertisement. It can occur in some program or in applications with free licence. An advertisement can be displayed in some banners or pop-ups. It is important to note that the user may or may not agree due to the license agreement (EULA - End User License Agreement) with the installation of this type of malware. Data are not sent over the Internet unconsciously. [5]

3.2.1.5 Spyware

Spyware sends user's data over the Internet unconsciously. In a better case sent data are called "static". It could be a record of visited sites and installed programs. These data could be used for a targeted advertising. In worse case these sent data are called "vital". It could be the content of electronic wallets, online store certificates, passwords etc. [5]

3.2.1.6 Browser Hijacker

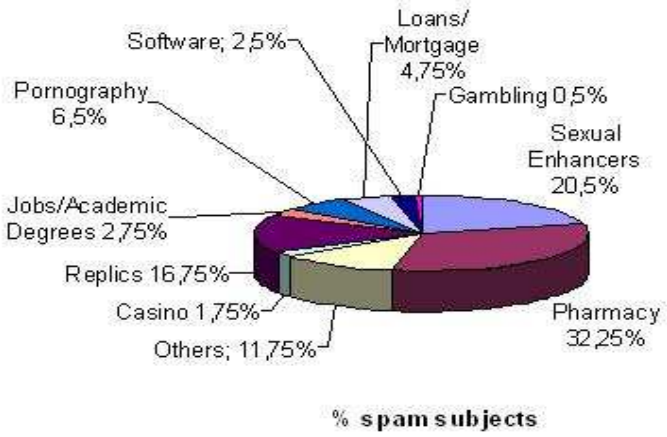
A Browser Hijacker is a special type of spyware. A Browser Hijacker is malware which changes a home page, an error page or a search page for another page created by author of browser hijacker. In many cases this page contains advertising and the owner of this page can have a profit made by a visit rate. [5]

3.2.1.7 Spam

The spam is not considered to be malware if there is no malware application. The spam could be just an unsolicited message about advertising. Nowadays, it can also appear in discussion forums, comments or instant messaging.

If no high-quality spam filter is applied, then the mail box can be overloaded and it can be very difficult to work with e-mails, which are not spams. [5]

Fig. 4: Types of spams



Source: http://farm4.static.flickr.com/3335/3234535186_73ab4c31b6.jpg [cit. 2009-01-28].

3.2.1.8 Hoax

A hoax is a kind of a spam without targeted advertising. A hoax could be called an alarming report and it notifies of non-existent threats. The aim of a spam is sending messages to all friends or colleagues. The hoax is not dangerous if e-mail recipient knows that information is false. A hoax can make a profit for an Internet provider. If recipient decides to download an e-mail with a subject “really important message” from some friend, he has to pay for that in case of some special Internet tariff. And it could be more than one e-mail per day.

There is an opportunity to visit a website with the database of hoax which is actualized every day. [5]

3.2.1.9 Phishing

Phishing is a forgery of e-mail messages. Recipient can be easily deceived because in many cases the message seems to be sent from some significant institutions, usually banks or savings banks. The recipient is referenced to a prepared form, which appears in the environment of a particular corporation. After click, a recipient is

redirected to a foreign server, where the attacker is able to get the entered data. It can be an account number, PIN of credit card, an access to internet banking, etc.

The fight against phishing exists on several levels. Programs allowing a detection of these attacks and report on them could be used. There are organizations fighting against phishing in order to remove these sites. [5]

3.2.1.10 Rootkit

Rootkit is a program that allows an attacker to hide their activities. Rootkit tries to hide directories and files, processes, network and system services, particular registry entries etc. Detection of the anti-virus program is not always hundred-per-cent and special programs are recommended to reveal it. [5]

3.2.2 Employees

Many types of malware are known but when an employee is cautious and behaves by rules there is a low possibility of data security accident.

In case an employee is not careful of personal and company data or personal and company property possible threats can occur. [1]

3.2.2.1 Identity theft

"Identity theft is a type of fraud which involves stealing money or gaining other benefits by pretending to be someone else. Having your identity stolen can be both financially and emotionally devastating. Identity theft can occur in many ways—from somebody using your credit card details illegally to make purchases to having your entire identity assumed by another person to open bank accounts, take out loans and conducting illegal business under your name." [15]

There are 5 types of the identity theft: business/commercial identity theft using another's business name to obtain credit, a criminal identity theft posing as another person when apprehended for a crime, a financial identity theft using another's identity to obtain credit, goods and services, an identity cloning using another's information to

assume his or her identity in daily life and a medical identity theft using another's identity to obtain medical care or drugs. [14]

Personal information could be readily available from cards in a wallet, e-mails, public records, information saved in the computers, information posted on social networks and many other places.

Scammers can easily acquire information owing to the human inattention or the carelessness. Situation when employee’s wallet or personal computer is stolen can occur. It could be also a situation when employee gives his data to unauthorized person unconsciously. Phishing scams, a phoney fraud alerts or false job opportunities can occur as well.

Warning signs exist and employee should know them. An e-mail, SMS or phone call asking to validate or confirm banking details can represent them. There are amounts of money missing from bank account without some reasons. An impossibility to obtain credit or a loan because of an inexplicably bad credit rating can represent it as well.

Several rules for a protection of the personality have been made. Not to give personal details to unknown and unreliable people in case of a phone call from a bank or any other institution. It is necessary to ask about a name and a contact number and to check the web pages or documents from these organisations before calling back. Not to use links or phone numbers of a received e-mail from any institutions. Regularly check a credit card or bank statements to ensure, that suspicious transactions are detected. Not to share all documents containing the personal information, such as credit card applications and bank statements. To log directly onto websites interested in rather than clicking on links provided in the e-mail. [15]

3.2.2.2 Hardware and software drawbacks

As mentioned earlier the computer could be stolen. Information is stolen physically when all computers or just a data media such as external hard discs, flash discs, CDs or DVDs, a floppy discs or some documents with personal details are stolen by any person.

It is a duty to act in such a way that information should be protected by a password, protected by mechanical devices such as lockable boxes or protected by mishandling by an employee or a server administrator.

3.3 Security features

When we are informed about possible threats we have got this advantage to preserve our data from the data loss or data damage. Many software means of protection and advice for employees are presented in order to inform how to avoid it.

3.3.1 Network security

Network security is a protection of hardware and software devices. Computer network is a group of two and more computers and these computers are connected together and mostly to the Internet. Possibilities of threats are evident and therefore the network must be protected. We can protect our network with special software means, the hardware means have to be high-quality and employees have to be educated. [4]

3.3.1.1 Passwords

Password usage is one of the best solutions how to avoid the data loss or data damage. Passwords are used in case of logging to applications. Password as a way to log into the computer operating system, to log into some applications and programs, to log into our mail box or log into some social networks.

Rules are required in order to protect data security. We can find many basic rules about correct types of password. Companies can also establish their own rules. [3]

3.3.1.2 Antivirus

An antivirus keeps track of all the most important inputs or outputs in an operating system where it is a possibility of not even virus attack. It means every possible malware can occur.

A group of antivirus programs consists of on-demand scanners which are used if there is no possibility to run an operating system by standard method and the subject

antivirus programs which are used to detect and remove one concrete type of virus. Antivirus programs are created and used in time when virus appears.

Antivirus system as a complex antivirus solution means a tool protecting computer systems against worms expanding by e-mails. It also prevents from download of maleficent files and it has many other functions. This complex program can include a firewall and other specialise tools.

Antivirus searches and checks the data according to virus database. This database has to be updated every day because there is new or changing malware.

There are many options of antivirus programs. It could be freeware, shareware or a trial version. [5]

There is a comparison of the most widely used antivirus programs.

Fig. 5: Comparison by Antivirové centrum

Antivirus program	Number of tests	Successful	Unsuccessful	Percentage of success
Microsoft ForeFront	11	0	11	100,00%
ESET (Nod32)	63	3	60	95,30%
Symantec Norton	59	7	52	88,20%
Avira	25	5	20	80,00%
Sophos	66	16	50	75,80%
Kaspersky	67	17	50	74,70%
F-Secure Anti-Virus	54	15	39	72,30%
CA eTrust	54	15	39	71,50%
Norman	62	19	43	69,40%
TrustPort	13	4	9	69,30%
BitDefender	29	9	20	69,00%
McAfee	64	21	43	67,20%
Microsoft Security Essentials	3	1	2	66,60%
Avast!	57	23	34	59,70%
AVG	52	22	30	57,70%

Source: http://www.antivirovecentrum.cz/aktuality/srovnani-antiviru.aspx [cit. 2010-09-21]

3.3.1.3 Antispyware

Antispyware is a program for detection and removing spyware.

A favourite antispyware is Spyware Terminator. This program is similar or better in many functions than other antispyware programs. It is freeware.

There are four types of verifications: the fast verification which scans important parts of an operating system as running operations, libraries, and cookies, then the optional verification when every user can chose what will be checked, the complete verification as a heuristic analysis which should find malware helped by ClamAV antivirus, and the last is a scheduler when every user can set the automatic verification in a specific time.

There is an effective removing of threats, an automatic removing of selected objects at the start of operating system and quarantine.

The residential shield is a constant operating system protection against all possible threats and uses ClamAV antivirus and Host Intrusion Prevention System.

There are also other useful tools. There is recovery of system settings, an analysis of a selected file and removing of locked files.

This program has to be updated. We can set the manual or the automatic update. [5]

3.3.1.4 Firewall

"*A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria."*[13]

There are several types of firewall techniques:

- *Packet filter: looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly*

effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.

- *Application gateway: applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose performance degradation.*
- *Circuit-level gateway: applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between hosts without a further checking.*
- *Proxy server: intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.*

In practice, many firewalls use two or more of these techniques in concert. A firewall is considered first line of a defense in protecting private information. For higher level of security, data can be encrypted. [16]

3.3.2 Encryption

Encryption is a method how to protect information which is sent or stored. Ciphers are based on mathematical principles and dependent on high power computers. So nowadays, everybody can use encryption.

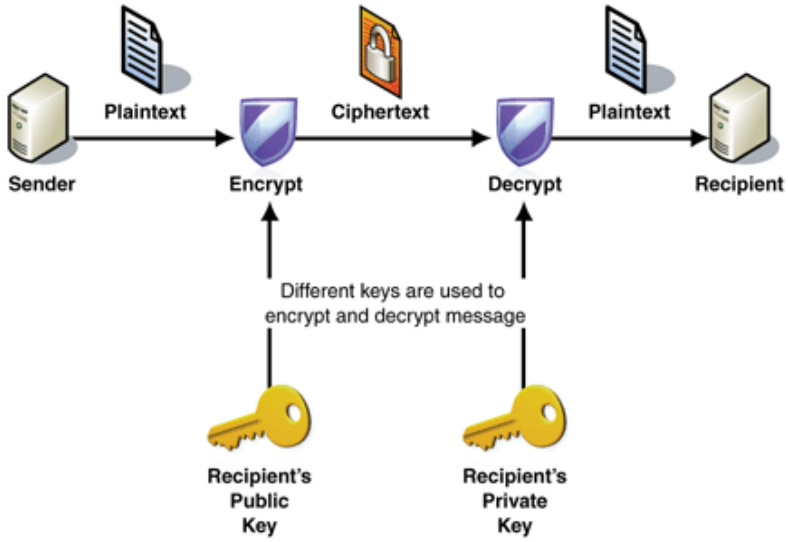
Users do not cipher the data. Data encryption is implemented by computers. There is a rule for encryption that costs of decryption by an attacker must be higher than an attacker profit in the case of successful decryption.

Two types of encryption are known. There is symmetric and non-symmetric encryption.

Symmetric encryption is easier than non-symmetric encryption. It does not need so high power computers and the procedure of encryption is easier. It has arisen much earlier than the non-symmetric encryption. Same cipher key for an encryption and a decryption has been used.

Non-symmetric encryption is a way when every participant has two cipher keys. One key is for encryption and the other one is for decryption. One key is called public key and other one is called private key. [6]

Fig. 6: Process of a non-symmetric encryption



Source: http://i.msdn.microsoft.com/dynimg/IC21919.gif

[cit. 2011-03-24]

3.3.3 Backup

A backup means to make a copy and save this copy of our data on some data medium. We can execute a complete backup of all files, a backup of select files or we can execute an incremental backup. An incremental backup is a copy of files which were changed and the copy of new files from the last backup. In the case of a backup some data memory is required. As memory data media as CD, DVD, an external disc or an online storage could be used.

There are several backup methods. A manual backup is an easy solution with low costs but user has to keep in mind a regular repetition of this operation. An automated backup, which is a planned action, and special backup software has been offered for free. This software can establish where and when data should be saved.

Compression of a data copy could be executed in these cases as well. A tool to make a compression of data and also decompression has been required, if we need to use these data again. Some software is for free but the better software which is used in many companies is paid.

The most frequent question is how often is necessary to make backup. It depends on an importance of data and how often data are changed or new data are made. Backup could be performed every day or every week or in order to delete these data from some data space. [12]

3.3.4 Data Recovery

If data are damaged or lost in some way recovery is a possibility how to get data back.

If data were deleted by mistake, software for free or paid, which can recover our data, has existed. Just in case that data were not overwritten. If data medium was damaged many companies offer an operation of data recovery.

There is an advantage of backup. There is nothing easier than use this data copy. So it means to follow the rule about a backup.

3.3.5 Archiving

Archiving is not the same as a backup. There are 2 cases of archiving. Archiving of data which we have not used for a long time has been executed. Second case has been a demand of space on expensive data storage. The difference between a backup and archiving is that there is a data copy and this data copy is stored on the other place. This process is performed by a reason of data security. During archiving no data copy has been generated. Data are transferred on the other low cost data media.

If company lost important data it could be a reason of company expiration, so backup is really necessary operation. On the other hand if company lost archived data it means that data are not so important and that is the reason why these data were archived. There are also some rules why data must be archived for some time. [9]

3.3.6 Duplication

Quite interesting method is a method of duplication. Data are saved on two data media. This method is obviously twice expensive and the data manipulation is slower. [2]

3.3.7 Removing unnecessary data

Sometimes it is necessary to remove data because of a need of a memory or when data are not needed any more. It is necessary to decide what to do. Some data could be really sensitive that's why a specialized method to remove them is required. Some companies create useful programs for this case. The best choice is overwriting of a memory.

3.3.8 Tips to prevent data loss or damage

"Use Antivirus software and keep it updated.

Antivirus is designed to protect you and your computer against malicious computer virus. Some virus infections can delete, modify your data secretly and cause your computer to crash. So be sure to update your Antivirus software with the latest patch and signature files for maximum security.

Protect against power surges with an UPS

An uninterruptible power supply protects your computer and data during a power surge or failure. The spare battery in the UPS gives you ample time to save your documents and shut down Windows properly so that you don't lose any files or damage any hardware components.

Keep your machine in a dry, shaded and dust-free area

Never leave your computer near places where it is directly exposed to rain, sun or humidity. Such conditions have the tendency to cause rusting and damage to your hardware parts.

Do not attempt to repair or open up your computer without assistance

Without experience, you may damage the circuit boards, hardware components and worst of all, receive a nasty electric shock! Always consult an expert.

Do not over-tweak your system

Avoid modifying your system registry or overclock your hardware to yield performance boost unless you're absolutely sure of what you're doing. You don't wish to fry your computer.

Store your backups at an off-site location

This helps to protect your backup from damage in case of a fire or disaster.

Avoid moving your computer when it is in operation

You definitely would not wish for your power cord to fall off and cause a data corruption and physical damage to your hard disk such as a head crash while working on a project.

Do not share access to your computer with strangers on the network

Your computer data can be prone to theft and modification if anyone on the network can access your files freely.

Practise disk maintenance

Clean up temporary files, unused files and defragment your hard disk from time to time. This helps to keep your hard disk on top form.

Read failure symptoms

You know it's time to start backing up all your data files when your hard disk starts producing funny noises and your system starts getting cranky." [11]

3.4 Standards, regulations and laws

4.3.1 Standards

4.3.1.1 ISO/IEC 17799

Information technology - Security techniques - Code of practice for information security management. This standard contains 11 basic safety sections, which are further divided into 39 categories of security. Security Policy, Security Organization, Classification and management of assets, Safety of Human Resources, Physical and environmental security, Management and Communications Management, Access control, Development, maintenance and expansion of information systems, Incident management, Business continuity management, Compliance with the requirements.

Each of these 39 categories includes safety objective (control) measures, which determines what is to be achieved and one or more measures that can be used to achieve the required action. The standard contains a total of 133 "basic" measures which break up into hundreds of specific security measures.

Objective measures provide a good basis for developing a set of "axioms" for security policy. The standard does not mandate that measures must be strictly applied, but leaves the decision on the organization. Appropriate measures are selected on the basis of a risk assessment and their implementation is dependent on the particular situation. The aim is to implement everything that describes the standard, but rather aims to meet all applicable measures. This approach ensures that the standard is widely applicable and gives great flexibility in an implementation to users.

4.3.1.2 ISO/IEC 27001

Information security and ISO / IEC 27001 are not just about information technology. As systems of quality management systems, environmental management systems or a health and a safety at work, an information security management system includes a management, a policy, an organization and a regular review.

- ISO/IEC 27001
    - Information security is an integral part of the whole of the organization
    - Main factors affecting business competition, information and security are in a controlled mode
    - Support the reliability of backup systems
    - Employees are responsible for the information security of their workplaces and their customers
    - Requirement for continuous improvement ensures effective management of long-term costs

Criteria for this certification is a total unknown, certification may still be proceed in several successive situational audits, which are also lessons and training for a company , particularly in the following areas:

- Analysis of the value of their assets in the field of the information

technology

- Risk analysis in relation to information
- Information Risk Management

The part of training is the training analysis and risk management. There is also a declaration to ensure about information security and other procedures.

- ISO/IEC 27002 Code of Practice
  - description of safety objects and instruments for their achievement
- ISO/IEC 27003
  - reserve for future guidance for the implementation
- ISO/IEC 27004 - Information security management metrics and measurement
  - specifies what and how to measure for identifying and describing the effectiveness of the ISMS constructed in accordance with ISO / IEC 17799
- ISO/IEC 27005 - Information Security Risk Management
- ISO/IEC 13335 - Management of information and communications technology security
  - the concepts and models underlying understanding of IT security
  - the risk analysis techniques
- ISO/IEC TR 15945 - Specification of TTP services to support the application of digital signatures
- ISO/IEC TR 18043 - System deployment operations of intrusion detection systems - IDS
  - The technical report with the methodical instructions how to incorporate ITS into the IT infrastructure
- ISO/IEC TR 18044 - Information security incident management
  - The technical report about the methodical management of security incidents

4.3.2 Regulations

The most important EU legal regulations on information security are:

- 1997/66/ES Data Protection in Telecommunications
- 1995/46/EC Protection of personal data
- 2002/58/EC Processing of personal data and privacy in electronic communications
- 1999/93/EC About conventions of Community framework for electronic signatures
- 1991/250/EEC Legal protection of computer programs

4.3.3 Laws

According to legislative terms Czech Republic have no special law that comprehensively solves the security of information technology. Many key laws are confirmed:

- Act No. 148/1998 Protection of classified information
- Act No. 101/2000 Protection of personal data
- Act No. 106/1999 Free Access to Information
- Act No. 151/2000 Telecommunications
- Act No. 227/2000 Electronic signature, including implementing regulations
- Act No. 365/2000 Public administration information systems
- Act no. 480/2004 Some information society services

Manipulation of certain categories of sensitive information directly is regulated by other laws:

- Act No. 513/1991 Commercial Code solves the issue of commercial confidentiality

  Act No. 89/1995 State Statistical Service, which regulates the safe handling of information, provided by natural and legal persons for statistical purposes
- Act No. 344/1992 Cadastre Republic (Land Act)
- Act No. 133/2000 Public Administration figures

- Act No. 455/1991 Trades (Trade Act)
- Act No. 337/1992 Administration of taxes and fees.

It is according to [8].

3.5 Safety audit

"Audit of information system is a process which is concerned with an assessing and a consultancy of objects in an environment where information technologies are used."

2 known methods of an audit which are international and have a general character as an instrumental to a creation of specific methods are ISACA - COBIT (Control Objectives for Information and related Technology) method and INTOSAI - IS (International Organization of Supreme Audit Institutions - Information Systems) method.

There is a possibility to ask for a realisation of an audit. Many specialized companies have offered it. [7]

3.6. Safe company

If the company is safe, the company data are also safe. It is necessary to define when the company is safe. There are some conditions.

Firstly decision as who is a responsible person which cares about this important part of company system has been made. Many people think that this problem is just about computers so some IT (Information technology) employee should inspect it.

The director of IT department is CIO (Chief Information Officer), which is partly responsible for data security. It also depends on a size of a company. Some small company does not need an employee responsible for this part of system. It is better to use a possibility of external provider. These people are much more specialized and costs are similar. Some greater companies have a responsible person or a responsible team which inspect just the security.

CISO (Chief Information Security Officer) is a person which is subordinated to CEO (Chief Executive Officer). CISO and CIO are at the same level in the company.

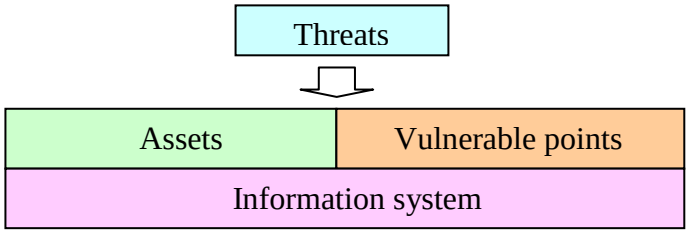
They have some implementing powers. But in many really great companies there is a security department and IT department is mostly subordinated to CISO.[2]

3.6.1 Security policy of a company

Some form of written document where are rules and answers about questions as what to protect, why to protect, how to protect, how to check that there is a proper security, what to do when something goes wrong has been made in the company related to a security policy.

Firstly data which are required to be protected and which are placed in the company have to be selected. Then threats have to be identified, vulnerable places and emergency plans of the company as well.

Fig. 7: Assets and threats

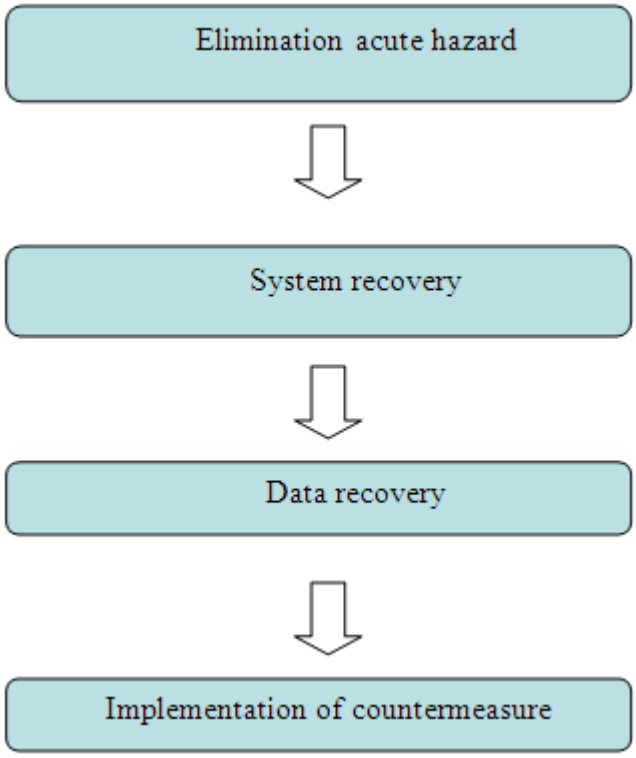


Source: DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat.

A risk analysis consists of three steps: resource identification, a threat identification and risk analysis of a company. After all that proper protection could be selected.

If there is some problem company has to behave according to emergency plans and CISO is responsible for a following problem solution. The whole process is depicted in a scheme. [2]

Fig. 8: Emergency plan



Source: DOSEDĚL, Tomáš. Počítačová bezpečnost a ochrana dat.

3.6.2 Personal and administrative security

Importance is a personal and an administrative security. It is necessary to observe a proper behaviour to employees, a life cycle of employee etc. Everything must be determined in all company processes, directives and regulations.

Every employee has some life cycle in a company. An employee is situated in many phases during the time. The beginning is an arrival at work and the end is a closure of the work agreement. It has to be determined what exactly employee has to know about security rules and this employee has to sign an agreement that he was educated. An employee has some access privileges which are set up by an employee of IT. If an employee is leaving company he can have some obligations towards this company. An employee keeps all information according to a secrecy agreement.

It is useful if there is specialized safety training for employees. Many times this training is performed by an external company. It could be a meeting or an online material. It has to be designed especially for every company according to needs and conditions.

There are some directives and regulations. The aim of these documents is how to solve some problems. Every document has an expiration date and it could be different for every department of the company. It could also contain different rules for every department of the company. These documents have to be designed by an internal employee who knows this company so well and can include everything what is important in the documents. [2]

4 Analysis of data security

The description of analysed companies is focused on the basic information about the company and its data security.

The analysis of data security contents following information:

- security of a safety audit (if it is provided)
- security of a physical access to data media
- security of a logical access to data
- security of saved data
- data security against data damage

This analysis is based on the description of data security according to the book Computer security and data security from Tomáš Doseděl. Information was provided by members of the company within the interviews and questionnaires. Questionnaires are filled by 60 employees of every company and interviews were made with a responsible employee to data security in the company.

4.1 Introduction of companies

Three Czech companies are significant in their field of activities and companies' services are used by thousands of people. Real names of companies are not mentioned because of a protection of information which was provided to this diploma thesis. Companies are named LARGE, MEDIUM and SMALL. The company SMALL has least number of employees and company called LARGE has most employees.

4.1.2 Company LARGE

This company is one of the largest providers of communication services in a whole Europe. A Czech branch of this company was founded in the nineties of 20th century and more than 7 million customers use services of this company. The consolidated net profit was 12.28 billion CZK.

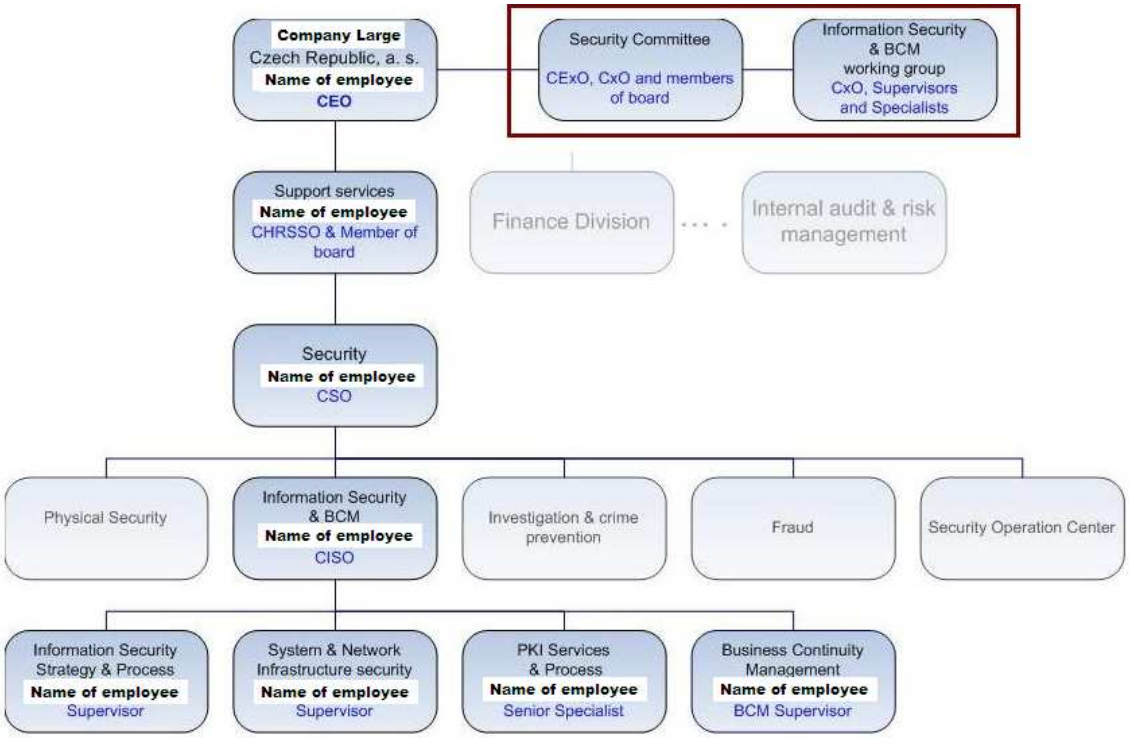
This company employs 7000 skeleton staff and 2000 external employees and owns many buildings in the Czech Republic which are on hand of this company or

tenanted. Two central buildings, where most information is saved and main people of management and other departments work, are in the capital city. It counts approximately 3000 employees.

Almost every employee has at least one computer or a notebook or both. It depends on a job position. Employee uses many applications for the data manipulation. These data are data of costumers or company data so it means that every careless data manipulation can be a cause of a criminal sanction or a financial penalty.

The structure of the security team is following. There are 13 employees in two teams.

Fig. 9: Structure of security team



Source: Material from company LARGE

The company has the local network in the building and use an Internet connection. There is an Intranet and WiFi in this company. The training about an information security for employees which is done by a virtual university is prepared. An online

application as a course where the employee has to go through and pass a final exam is required. This way is successful because this company announces an annual improvement. For now this company announces 90% of a success at passing a test.

4.1.2 Company MEDIUM

Dutch company was founded in 1877 in Vendlo, where the central building is still situated. The company production is based on an own research and development. This company invests approximately 7% of an annual sale in this research and development. Nowadays, company owns over thousand patents. There are more than 21,000 employees and about 1800 employees are focused on research and development.

Company offers comprehensive integrated solutions for working with documents based on a professional production hardware (copiers, printers, multifunctional systems, scanners), a complex system of sophisticated software for managing the Document Flow OMS and DMS, professional services (PS - "Professional Services -consulting, analysis, consulting, training ...), business services (outsourcing work with the document), reliable services, flexible financial services and to offer a wide range of consumables.

The basic philosophy is selling of services exclusively by its own employees. The main reason is to create relationships with customers and to understand their requirements. This company is a multinational company with an annual sale more than 3.3 billion. It currently operates branches in 35 countries and more than 80 countries cooperating with the dealers or distributors.

The Czech branch was founded in 1991. Today this company employs over 870 workers. It is the only global manufacturer of some reprographic equipment(hardware and software), which directly invests in a research, development and production within the Czech Republic and is also only European company having launched its own production (Prague, Pardubice) in copying and printing techniques.

The surveyed branch of this company is situated in Prague and 250 employees work there. There is an external company which performs services of an information technology therefore this company has no security team and also no employee

controlling services within the company. This branch is managed from a central office in Holland and systems are centralized. The company has a local network in the building and use an Internet connection. There is no WiFi and no Intranet in this company. There is no training of employees in order to ensure data security.

4.1.3 Company SMALL

This company was founded in the fifties of 20th century. The company provides public bus transportation in one city of a central Bohemian region, the surrounding area and international lines. The company employs 112 employees, 72 of them use some computer equipment, and 65 of them use an internal information system and are connected to the local network. Property of this company is estimated at 100 million. The company endeavours after a long-term development and improvement of services through the transport service using computer technology.

Two employees and one security manager from an external company provide a whole maintenance of company's information system. These employees are not concretely specialised in the field of data security. The company has a local network in the building and use an Internet connection. Company uses no WiFi but Intranet is used in this company.

4.2 Security of safety audit

Safety audit is mostly realised by an external company. The objective of an audit is to find out which problems of an information security are and try to eliminate them. It is not a rule of every company to do this safety audit. But it is a great advantage to find out which drawbacks are and try to fix and improve it.

4.2.1 Security of safety audit in the company Large

The safety audit was realised for a whole information system of this company. Some parts are focused on data security. The safety audit was made by an external company in this manner:

- attempts at the limitation of services by breaking at the operating system level
- attempts at the limitation of services by breaking at the database application level
- attempts to obtain sensitive data

There were found some drawbacks within the case of data security:

- Remote execution of arbitrary code
- Weak encryption algorithms
- Out of date Certificate
- Poor security services

More IT audits are executed within this company. There is also an audit of internal audits.

4.2.2 Security of safety audit in the company Medium

No security audit has been executed yet for this Czech branch. Company has no information about a current state and possible problems.

4.2.3 Security of safety audit in the company Small

No security audit has been executed for this company. Company has no information about a current state and possible problems.

4.3 Security of a physical access to data media

As mentioned in part 3.2.1 Physical security it also should be analysed which way company protects data physically.

4.3.1 Security of a physical access to data media in the company Large

This company has many elements how to protect data physically. Every employee has an identification card. The main entrance of the building has turnstiles, where

employees have to use their cards in order to enter. There is a security guard monitoring a movement of employees and other visitors in halls due to the camera system. Security guard also can use other devices as scanners to check visitors and their luggage. Visitors are listed in an arrival-book.

Every door of every office has a special device as a card sensor where employees also have to use a card in order to enter.

New structure of company brings a new look of offices which is called “open space”. Every employee has a table and a personal small locker for documents. Just some managers and directors have offices.

A physical access to data means also a protection from fires, earthquakes, climate crack-ups and water crack-ups. This company has special rooms for information equipment as servers and others with securing components in order to ensure a protection from these problems. There is an air condition and fire alarm. This company has a standby supply.

4.3.2 Security of a physical access to data media in the company Medium

Every employee has an identification card. There is no security guard protecting main entrance, doors are equipped with a card sensor in order to enter the main entrance of the building and the main entrance of the company office. There is just a security service coming in case of an alarm. Monitoring system is used in order to make a recording. Nobody watches a situation in the company in a current time. Records could be retroactively watched. Visitors are not listed in an arrival-book.

This company has a special room where information equipment as a server and other devices are saved. This room is designed to keep a suitable climate. There is an air condition and a fire alarm. This company has a standby supply.

4.3.3 Security of a physical access to data media in the company Small

As previous two companies this company also uses an identification card system for employees. Some employees own special coded keys which allow entering just in some specific rooms. There is a main entrance with a security guard. Monitoring system

is not located in a whole company. Just one important part of company, where customers use services, is monitored. Visitors are not listed in an arrival-book.

A server and other equipment are located in a special room with an air condition. This company has a standby supply.

4.4 Security of a logical access to data

This part is focused on identification, authentication and the access control.

4.4.1 Security of a logical access to data in the company LARGE

Every employee has an identification number where the same number as an identification card number is written there. This number and also a password have to be used in every application. Many applications have been used in the company. Not every employee has an access for all of them. It depends on a position in the company. Employee has to apply for access privileges and access privileges to every application have to be confirmed by a competent supervisor. Then this application is reviewed by the security manager and access privileges are assigned or not.

The access of the computer operating system is reviewed and the system requires a proper form of password if there is a change. First password is generated and an employee obtains it from the security manager. This password is not required to be changed. The access of special applications does not review a proper form of password but every time an expiration date of password are displayed and after this time the password has to be changed.

The system of access privileges has been linked therefore there is a possibility of authentication for many application. User logged in operating system can use some operations with another login data and this situation has to be checked. It is a double protection.

4.4.2 Security of a logical access to data in the company MEDIUM

Every employee has an identification card with a number. This card is used in order to enter the building and to record the time when employee enters and leaves the

building. Employee uses own name and password in order to work with company applications. There is no name and no password required for an access of the computer operating system. There is no possibility of authentication in this company. Company applications are designed for every part of a working process. It is not necessary to solve access privileges because every employee has few possible operations which can be executed.

4.4.3 Security of a logical access to data in the company SMALL

Every employee has an identification card with number. This card is used in order to enter the building and to record the time when employee enters and leaves the building. Employee uses own real name and own password after first change of an initial password in order to work with company applications. No name and password are required for an access of computer operating system. There is no possibility of authentication in this company.

4.5 Security of saved data

4.5.1 Security of saved data in the company LARGE

Many employees work outside of the company building and all applications could be used via Internet. Employees need the company notebook where these applications are installed. Therefore it must be mentioned that data are brought up from outside of the company building. A secure remote access of employees has to be ensured.

Data could be modified by employees. It depends on access privileges and on a phase of a project which operations could be executed.

Company announces ISO certification. There is ISO 27001 certification from 1994 which is confirmed every year.

A method of an online and an offline encryption is used for necessary types of data. It is decided by internal norms of the company.

4.5.2 Security of saved data in the company MEDIUM

Data are brought up via data media by one company manager and IT management. A method of an online encryption is used for all data sent via Internet. Data are sent via network to a server and then these data are sent via Internet to a customer's server by SFTP. Company uses HTTPS to secure a connection between the web browser and the web server. Every employee could add new data but it is impossible to modify this data later. There is a possibility of a secure remote access of employees.

Company announces ISO certification, unfortunately no ISO certification for Information security.

4.5.3 Security of saved data in the company SMALL

There is just one person who uses a remote access to the company application. Data are brought up via data media as flash discs and special memory cards and there is no offline encryption. Data are sent via Internet to other companies. SSL/TSL protocol is used.

Company does not announce any ISO certification.

4.6 Data security against data damage

4.6.1 Data security against data damage in the company LARGE

This company has a specific backup plan. There are two centres where data are backed up. The distance between two cities is 70 kilometres. Process of duplication for specific type of data has been executed. Archiving is used in order to make a free memory of high efficient data media. According to law company have to execute process called anonymization. Data could be saved but without concrete personal details. Removing of data is not executed.

This company uses every possible feature against malware. Spam filter has a hundred-per-cent success. Company uses a system of firewalls, antivirus and antispyware from provider Symantec.

This company announced some problems of data security in the beginning of existing. Virus was spread in the local network by external employee's notebook connected to the company local network. The loss of an income was evaluated around hundreds of thousands.

There is a special hacker team that has an aim to find out if the system is sufficiently secure against possible threats.

4.6.2 Data security against data damage in the company MEDIUM

A backup is executed every day and a tape backup is executed every week when data are saved outside of the company. Duplication is executed by method RAID. Archiving is executed after a project finish via data media. Data are not removed. Just in case of a customer's request.

Company uses a firewall from a provider IBM, antivirus NOD32 from a provider ESET and the application against spam and spyware from a provider McAfee.

Company announces no problems of data security.

4.6.3 Data security against data damage in the company SMALL

A backup is executed regularly every month and just for some kind of data. There is no duplication and archiving. Data are removed in order to get free memory for new data.

Company uses antivirus from a provider AVG with a multiannual licence. SSL/TSL protocol is used for a data transfer. Applications as Spyware Terminator and Trojan Hunter are used in case of problems with malware. A spam filter is provided by an external company.

Company announces data losses from data media, a faulty function of a spam filter. That is the reason why IT manager declares an emergency and employees have to be beware of attachments.

5 Comparison of firms

An evaluation by Simple scoring method and SWOT analysis used to compare surveyed companies was made. SWOT analysis is used to evaluate a part of a research which is not possible to compare. There is just a part of SWOT analysis, concretely analysis of Strengths and Weaknesses as a research focused on internal factors. A Simple scoring method is used to evaluate questionnaires for employees.

Fig. 10: SWOT analysis

Source:
http://2.bp.blogspot.com/_I3Q1kT0tz2A/SFhpyxagADI/AAAAAAAABn8/KvtBYp6Di_c/s400/SWOT+chart.jpg
[cit. 2011-03-24]

5.1 Comparison of data security analysis

5.1.1 Security of safety audit (if it is provided)

No audits are executed in companies MEDIUM and SMALL. It is not possible to make a comparison. Just SWOT analysis was made as an evaluation of company LARGE which has executed IT audit every year.

Fig. 11: SWOT analysis of IT audit in the company LARGE

Source: Authors' source

5.1.2 Security of a physical access to data media

Company LARGE uses many protective means of a physical access to data media. Companies MEDIUM and SMALL use many of these means but some of them are used in a different way. For example let's focus on a security guard.

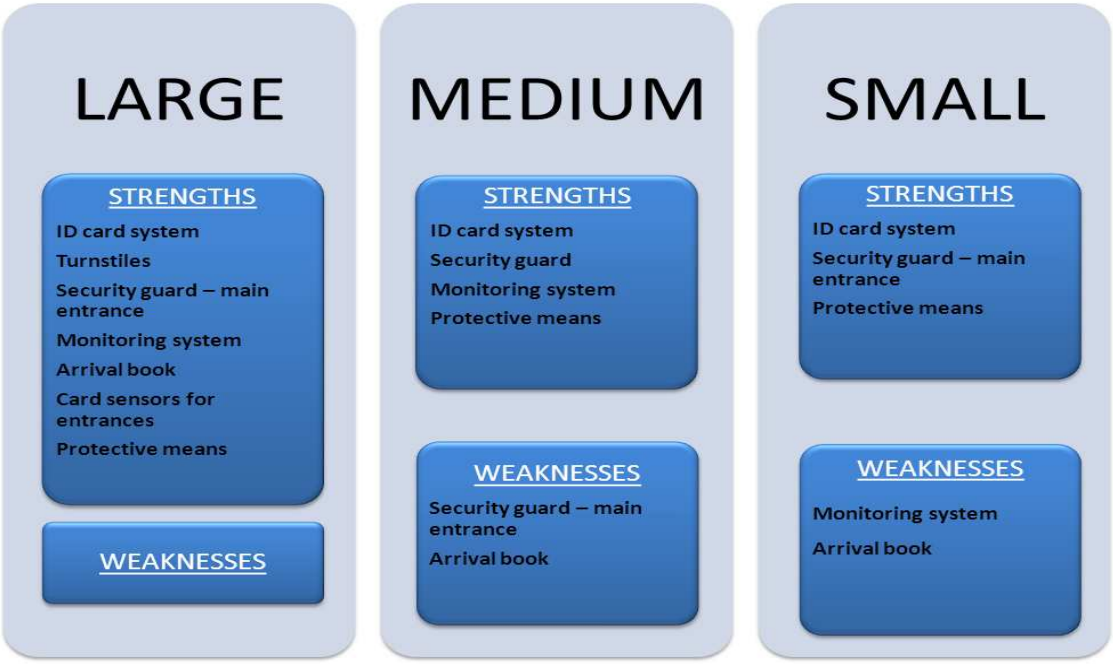
Company LARGE employs a security guard which is placed at the main entrance. This group of people monitors the company object in a current time. Security guard watches monitors and turnstiles, makes notes about visitors in an arrival book and scans their luggage.

Company MEDIUM uses a security guard of an external company which comes after an alarm call. There is a monitoring system but nobody watches a record in a current time. But there is a possibility to watch it by return.

Company SMALL employs 2 people as a security guard which is placed at the main entrance. There is no monitoring system watched and no arrival book about visitors.

The best solution in this case and also in total has the company LARGE. Then in many cases company MEDIUM uses better ways than company SMALL.

Fig. 12: Comparison of a security of a physical access to data media



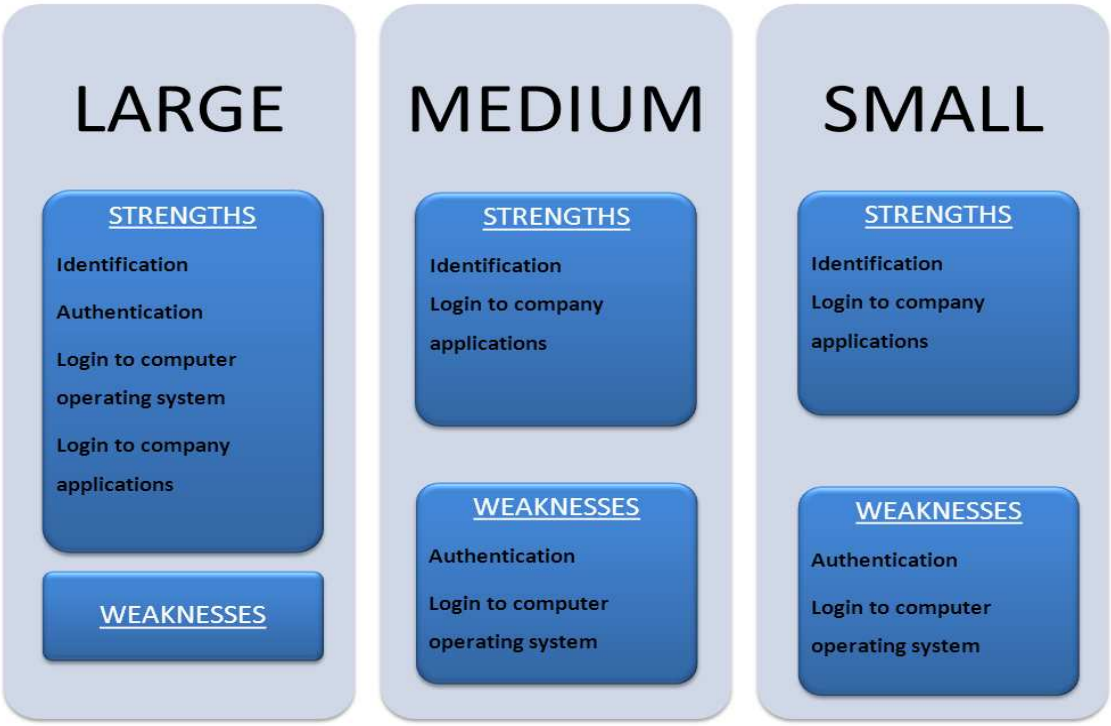
Source: Authors' source

5.1.3 Security of a logical access to data

Company LARGE uses 4 possible ways how to secure a logical access. The most important is a process of login to a computer operating system. That's the easiest way how to prevent from a direct access to data of an employee and a whole company.

Company LARGE uses best methods for this part of analysis. Company MEDIUM and SMALL solves this part of security similarly.

Fig. 13: Comparison of a security of a logical access to data

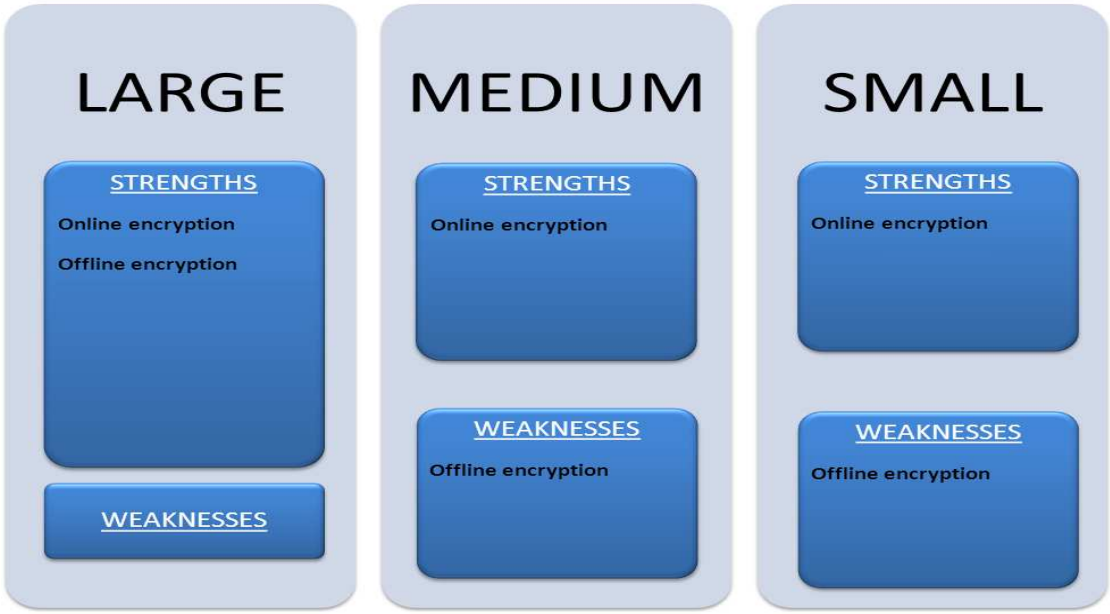


Source: Authors' source

5.1.4 Security of saved data

The same result as for a security of a logical access is for a security of saved data. Company LARGE uses both types of encryption and company MEDIUM and SMALL just one of them.

Fig. 14: Comparison of a security of saved data



Source: Authors' source

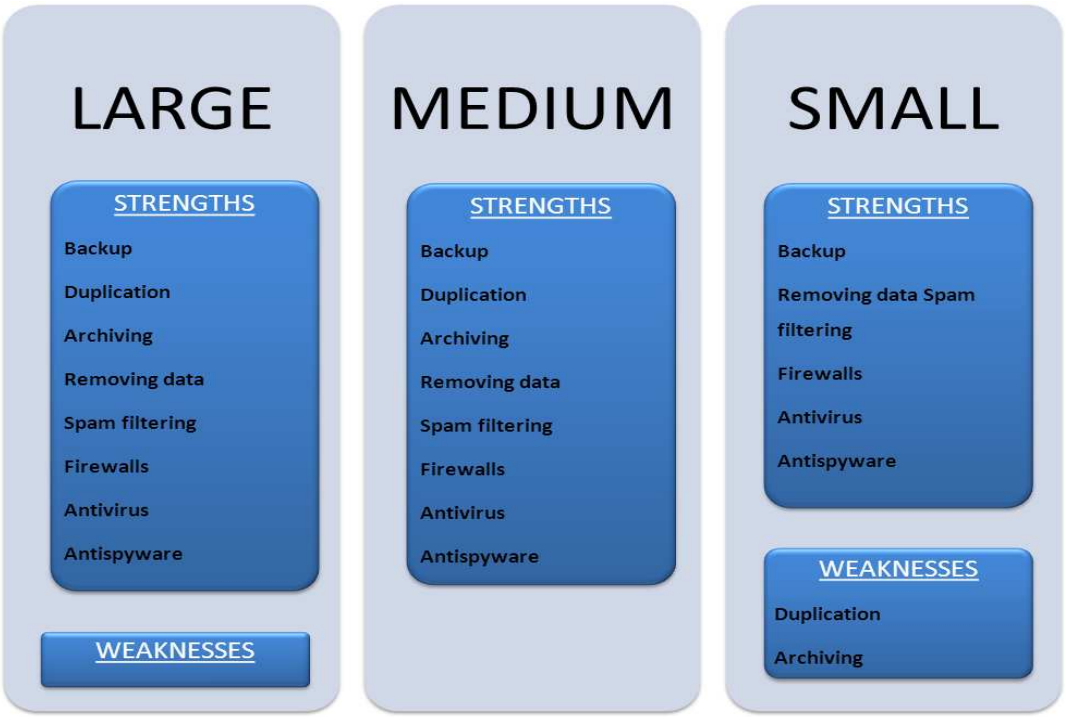
5.1.5 Data security against data damage

The company LARGE and the company MEDIUM cares about data security against damage similarly. These companies use many protective means but the quality of them is different.

For example all three companies use an antivirus. Company LARGE uses a complex solution for antivirus, antispyware and a firewall from a provider Symantec. The company MEDIUM uses an antivirus from a provider ESET. Company SMALL uses antivirus form a provider AVG. According to Fig.10: Comparison by Antivirové centrum - September 21 2010, the best solution of mentioned used providers is used by

the company MEDIUM, than the company LARGE and then the company SMALL. It is really difficult to decide which company has the best solution in total. It can be considered according to number of protective means that the company LARGE and the company MEDIUM have the same level of data security against damage and the company SMALL is also very well secured.

Fig. 15: Comparison of data security against data damage



Source: Authors' source

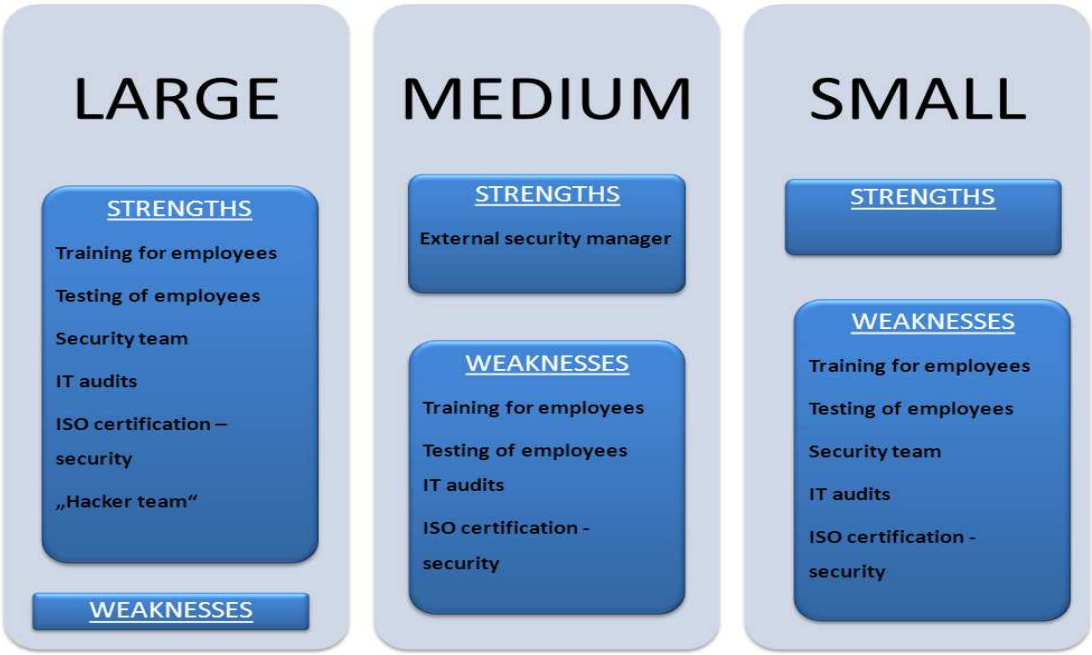
5.1.6 Data security - related information

It is evident that the best solution has the company LARGE. There is an efficient team of specialists which works in order to protect the company in a best way as it is possible. The useful way is for example a "Hacker team". These people try to make attacks in order to find out where weak points of data security are. IT audits are another possible way how to find out what is necessary to improve. Then the training of employees and testing them is a suitable way how to inform them about possible threats

and make them educated. ISO certifications are guarantee that company has proper solutions for the security.

There are no related advantages in the company SMALL and MEDIUM. Just the company MEDIUM uses services of an external security manager which is a suitable solution for this type of the company. If the company is smaller it is not necessary to employ an internal security manager. But it is still necessary to cooperate with a specialist.

Fig. 16: Comparison of data security – related information



Source: Authors' source

5.2 Comparison of questionnaires

60 employees of every company have answered 9 questions about password security.

Questionnaire

1. I use password in order to log into the computer operating system

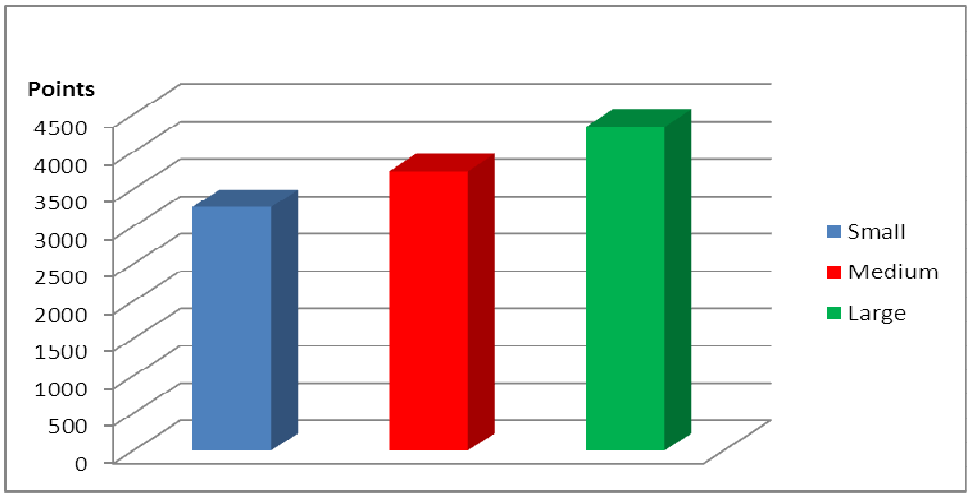
2. I use passwords in order to log into the company application and Internet applications
3. The number of characters of my shortest password
4. I use one of these possibilities in order to remember my password

(A name, a surname, a name of my family member or my pet, a nickname, a personal identification number, a periodic sequence of numbers, just one and the same character.)

5. My shortest password includes: (Write a number: the number of digits, the number of capital letters, number of small letters, number of other characters)
6. I betray my password to somebody
7. My password is written somewhere close to my computer
8. I change my password at least once per 45 days
9. I was cognizant of the facts of data security and other issues before signing a contract of employment or during the training

Results were evaluated by Simple scoring method. Every question was evaluated from 0 till 10. The best total result has gained the company LARGE as it is shown in a graph.

Fig. 17: Comparison of questionnaire results



Source: Authors' source

In more detailed analyses there is an evaluation of every question. See Supplement number 1. An arithmetic mean is used.

We can see that the company LARGE achieved the best evaluation of surveyed companies for all questions. For question number 4 there is the worst evaluation and the reason could be that employees have to use many company application. It means employees have to remember many passwords. Therefore they use the easiest way as a name of family member etc. how to remind these password.

Company MEDIUM achieved almost the same good evaluation as LARGE company for many questions. For some questions the evaluation is closer to the evaluation of the company SMALL. But it is totally the second-best result.

SMALL company achieved the worst result because mostly the result for any question was the worst one.

The online version of questionnaire is depicted in a supplement number 2.

5.3 Economic evaluation of costs for data security

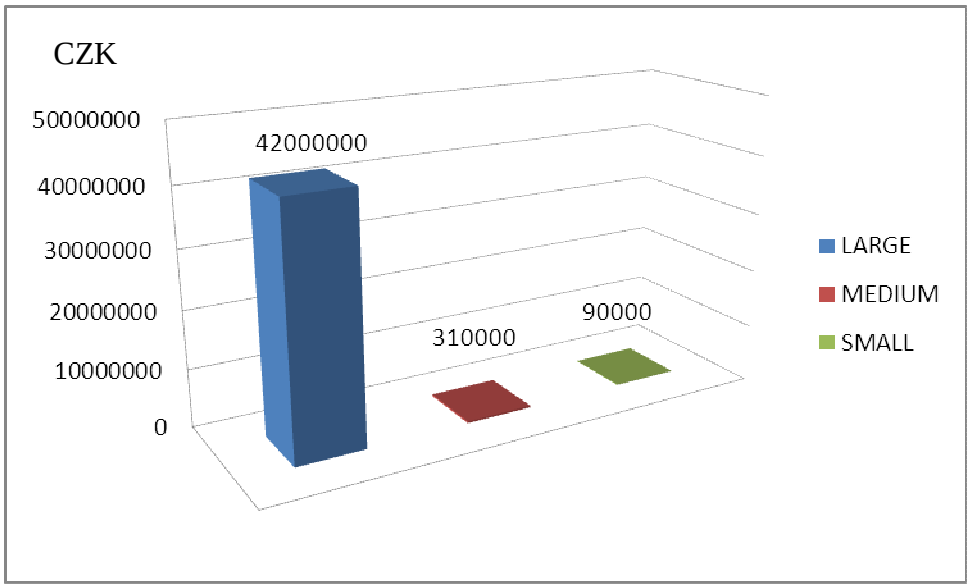
The graph depicts the costs made in order to ensure data security. It is evident that company which can invest a lot of money for ensuring of security achieves better level of security.

Company LARGE expends approximately 42 million CZK in order to protect data.

Company MEDIUM expends approximately 310 thousands CZK and the company SMALL expends approximately just 90 CZK thousands.

The calculation was made according to upon wages, protective hardware and software means, a monitoring system, a security guards, trainings, testing, audits etc. All means used in order to protect the data system.

Fig. 18: Costs of data security in CZK



Source: Authors' source

6 Conclusions

The hypothesis that the tested companies showed different results related to certain parts of the data security policies was proved, based on the performed analysis.. Company Large has the best solutions of data security out of these three companies. Company Medium and Small also try to take advantage of these solutions but their data security is weak in many ways.

The reason for these results is given by the differences in the company structure and processes. The main reason represents the budget available for ensuring the data security. In case the company could spend bigger amount of money to salaries, invest into purchasing of better software, education etc. then the data security level would be higher.

Company Large disposes of a team of specialists who have to ensure the data security. These employees are hired and motivated by a high salary. They are part of the company and they have responsibility for company data. It is recommended for a smaller company to hire an external security manager but this person does not feel such a high responsibility and loyalty because of foreign data source in comparison to the internal employee.

Employees of the company Large are educated thanks to the courses and tests provided by a virtual university. Thereupon the measure of data security is higher. Employees of companies Medium and Small attend no courses and pass no test. The data are in danger by lack of their training and awareness.

It is known that no information system may be fully secured. During an IT audit it was found out that even the company Large´s system has some drawbacks. The most significant drawbacks of companies´s Medium and Small system is that there has been no IT audit performed ever at all and therefore these companies cannot find out if there is something wrong which should be fixed or improved.

The software and processes which should serve to ensure the data security are selected by the level of the available budget as well as by the preferences and experience of the security manager. In these cases it is not easy to choose a cheap but at

the same time a purposeful and effective solution. However these companies work with sensitive data of their customers. They have to follow the law and therefore it is necessary for them to choose the best technology and processes to ensure the possibly highest security level.

I would say that my hypothesis has been proved. The different field of activity of these companies makes their different profit. Out of the total earned sum the company could invest more money for purchasing high-quality technology, efficient software and provide employees with valuable trainings. A company with high number of employees could have a higher probability of an error rate of employees. That is one of the reasons why it has to be paid more attention to the data security measurements in such companies.

7 Bibliography

7.1 List of quotations

[1] DOBDA, Luboš. *Ochrana dat v informačních systémech*. 1st edition, Praha : Grada Publishing, 1998. 286 p. ISBN 80-7169-479-7

[2] DOSEDĚL, Tomáš. *Počítačová bezpečnost a ochrana dat*. 1st edition, Brno : Computer Press, 2004, 182 p. ISBN 80-251-0106-1

[3]GOLLMANN, Dieter. *Computer Security*. 1st edition. Chichester : John Wiley & Sons, Inc., 1999. 336 p. ISBN 0-471-97844-2.

[4] BISHOP, *M. Computer Security. Art and Science*. 1st edition. Massachusetts : Addison-Wesley Professional, 2003. 0-201-44099-7 ISBN 0-201-44099-7.

[5] PFLEEGER, CHARLES; PFLEEGER, SHARI LAWRENCE. *Security in Computing*. 4th edition. New Jersey : Prentice Hall, 2006. 880 p. ISBN 0-13-239077-9.

[6] SALOMON, David. *Data Privacy and Security*. 1 edition. New York: Springer-Verlag, 2003. 469 p. ISBN-10: 0-387-00311-8.

[7] SVATÁ, Vlasta. *Audit informačního system*. 1st edition, Praha, 2005. 167 s. ISBN 80-245-0975

[8] BALCAR, Štěpán. *Bezpečnostní audit IT*. Brno, 2007. 59 s. Diploma Thesis. Masarykova univerzita.

[9] BLŠŤÁK, Oliver. *SystemOnLine* [online]. 2009-07 [cit. 2011-03-15]. Archivace. Available from WWW: <http://www.systemonline.cz/clanky/archivace-dat.htm>.

[10] KOLÁČEK , Michal. *Svět hardware* [online]. 2009 [cit. 2011-01-15]. Počítačová havěť - vývoj a rozdělení malware . Available from WWW: <http://www.svethardware.cz/art_doc-2E043BB4799DC37FC125755A005BC1EA.html>.

[11] LEONG, Jowyne. *PiciFix* [online]. 2006 [cit. 2011-03-15]. Tips to Protect Data Loss . Available from WWW: <http://www.picifix.com/computer-repair/ag7780.html>.

[12] *GenProxy* [online]. 2011 [cit. 2011-03-15]. Backing Up Your Data (Hard work) . Available from WWW: <http://www.genproxy.co.uk/backup.htm>.

[13] *Macaws Infotech* [online]. 2006 [cit. 2011-03-15]. Firewall . Available from WWW: <http://www.privacycom.org/content/release-4-cryptography/symmetric-and-asymmetric-cryptography>.

[14] *PEACEHOLD* [online]. 2010 [cit. 2011-03-15]. Identity theft & the Deceased. Available from WWW: <http://peacehold.com/2010/11/identity-theft>.

[15] *SCAMwatch* [online]. 2011 [cit. 2011-03-15]. Identity theft . Available from WWW: <http://www.scamwatch.gov.au/content/index.phtml/tag/identitytheft>.

[16] *WEBOPEDIA* [online]. 2011 [cit. 2011-03-15]. Firewall . Available from WWW: <http://www.webopedia.com/TERM/F/firewall.html>.

7.2 List of figures

7.3 List of abbreviations

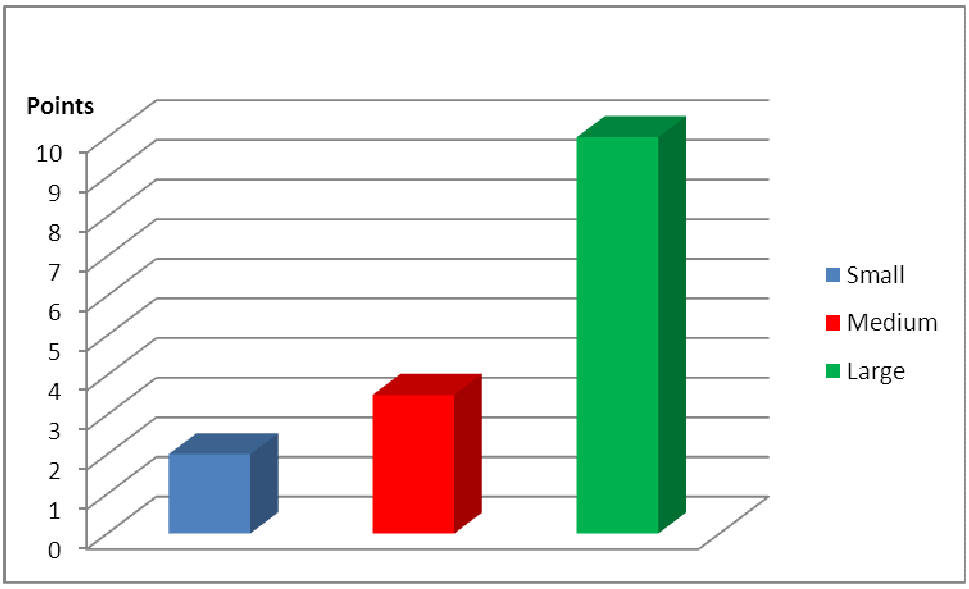
CD	Compact Disc
CIO	Chief Information Officer
CISO	Chief Information Security Officer
COBIT	Control Objectives for Information and related Technology
CZK	Czech Crown
DMS	Distribution Management System
DVD	Digital Versatile Disc

EC	European Commission
EU	European union
EULA	End User License Agreement
FTP	File Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ID	Identification
IEC	International Electrotechnical Commission
INTOSAI	International Organisation of Supreme Audit Institutions
IP	Internet Protocol
IS	Information System
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISO	International Standard Organisation
IT	Information Technology
ITS	Information Technology Services
LAN	Local Area Network
OMS	Outage Managements System
PS	Professional Service
SFTP	Secure File Transfer Protocol
SSL/TSL	Secure Sockets Layer/Transport Layer Security
SMS	Short Message Service
TCP	Transmission Control Protocol
TTP	Technology Transfer Programme
UDP	User Datagram Protocol
UPS	Uninterruptible Power Supply
WAN	Wide Area Network
WiFi	Wireless Fidelity; wireless technology based on the IEEE 802.11a/b/g/n technology

8 Supplements

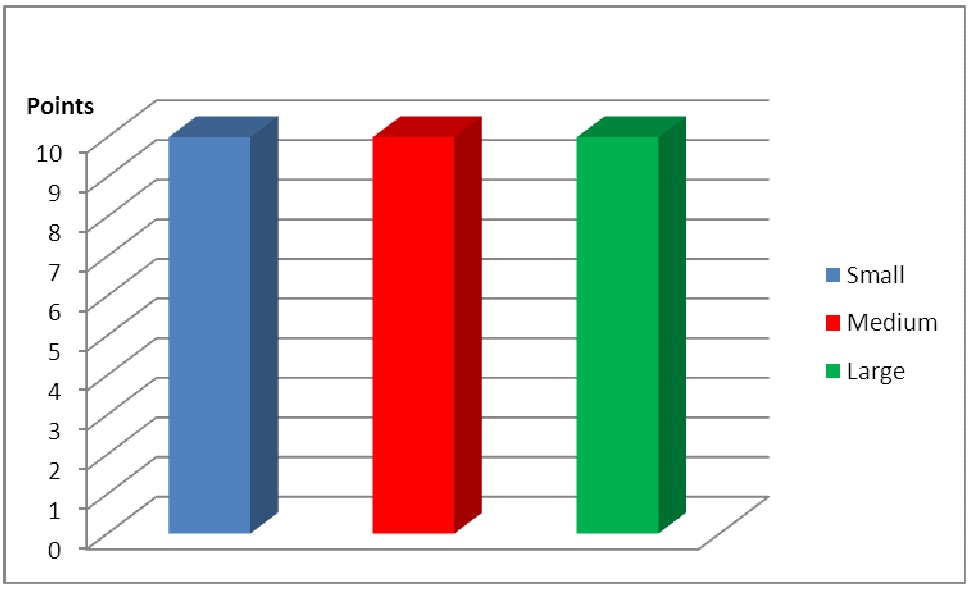
8.1 Supplement 1

1. I use password in order to log into the computer operating system



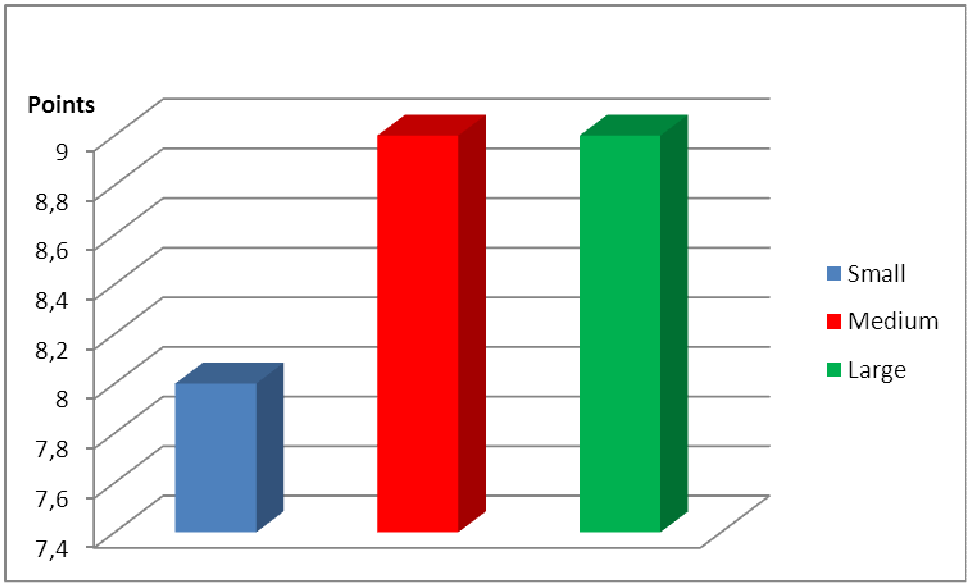
Source: Authors' source

2. I use passwords in order to log into the company application and Internet applications



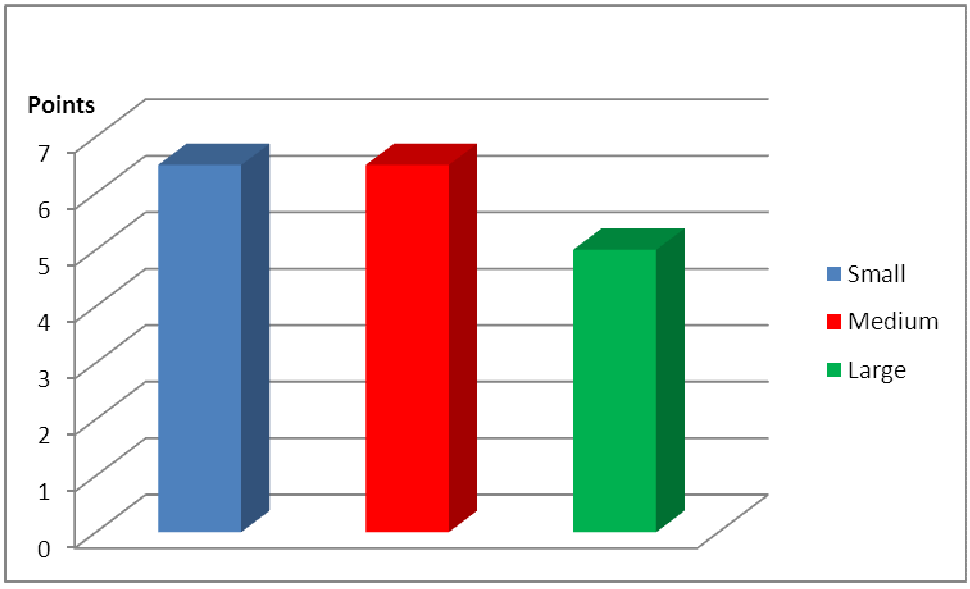
Source: Authors' source

3. The number of characters of my shortest password



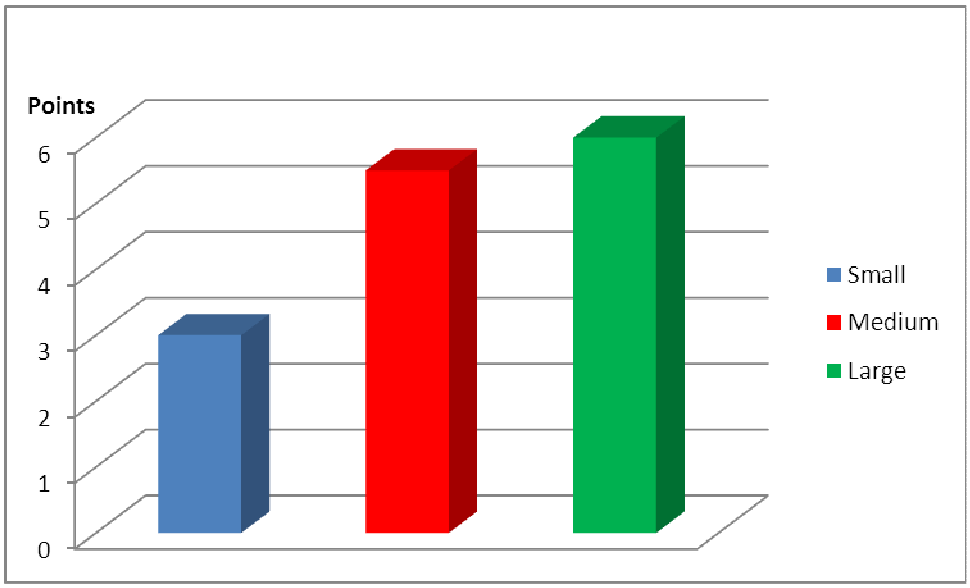
Source: Authors' source

4. I use one of these possibilities in order to remember my password (A name, a surname, a name of my family member or my pet, a nickname, a personal identification number, a periodic sequence of numbers, just one and the same character.)



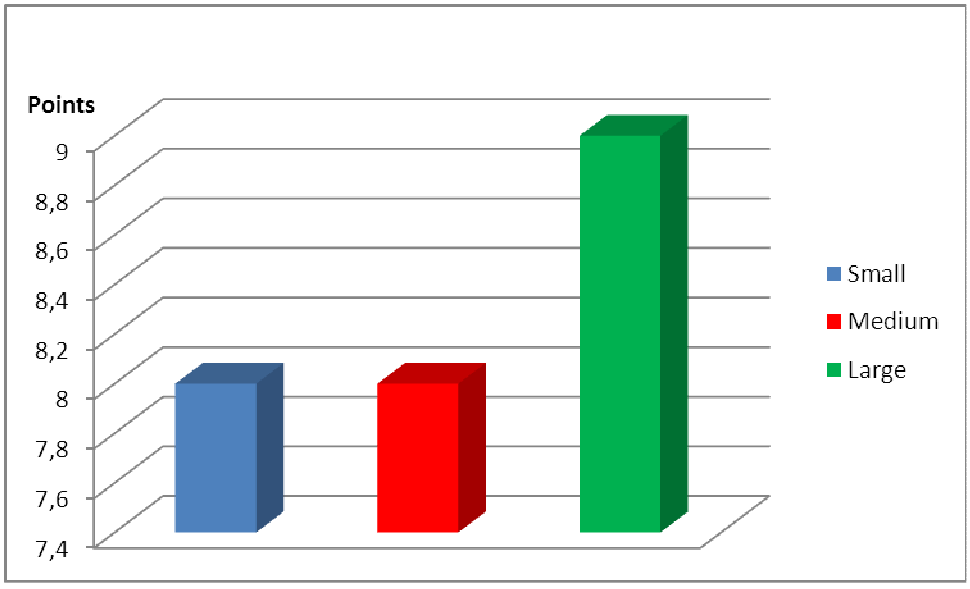
Source: Authors' source

5. My shortest password includes: (Write a number: the number of digits, the number of capital letters, number of small letters, number of other characters)



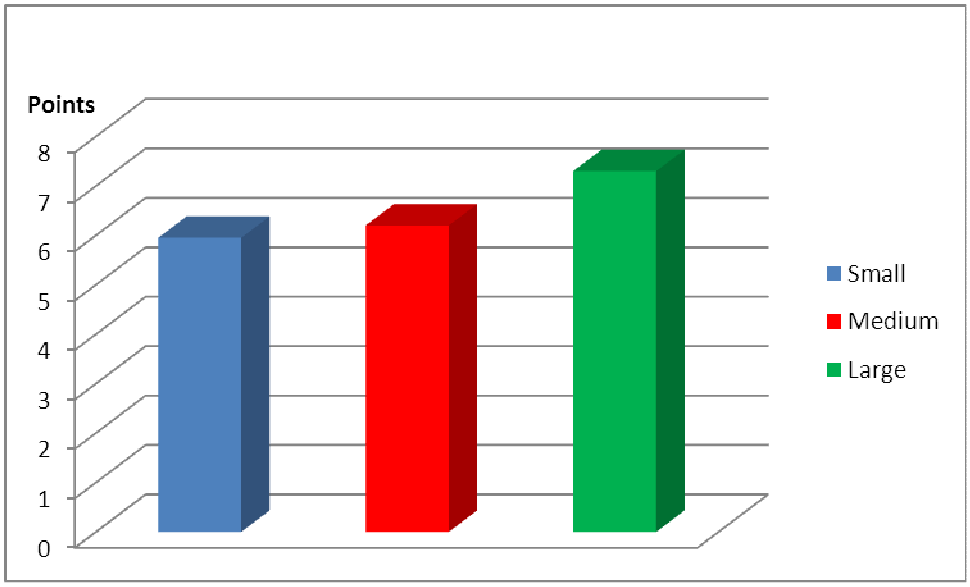
Source: Authors' source

6. I betray my password to somebody



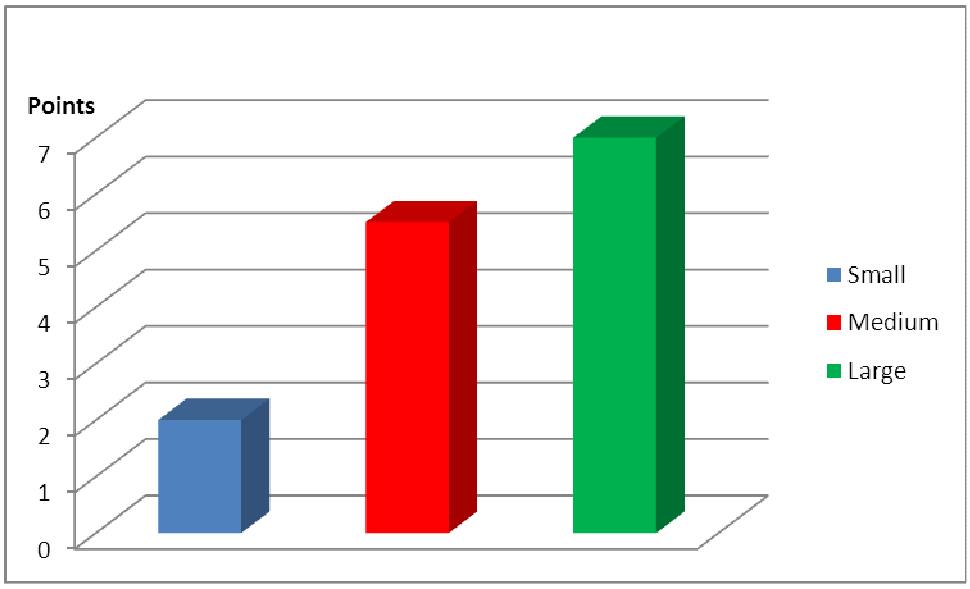
Source: Authors' source

7. My password is written somewhere close to my computer



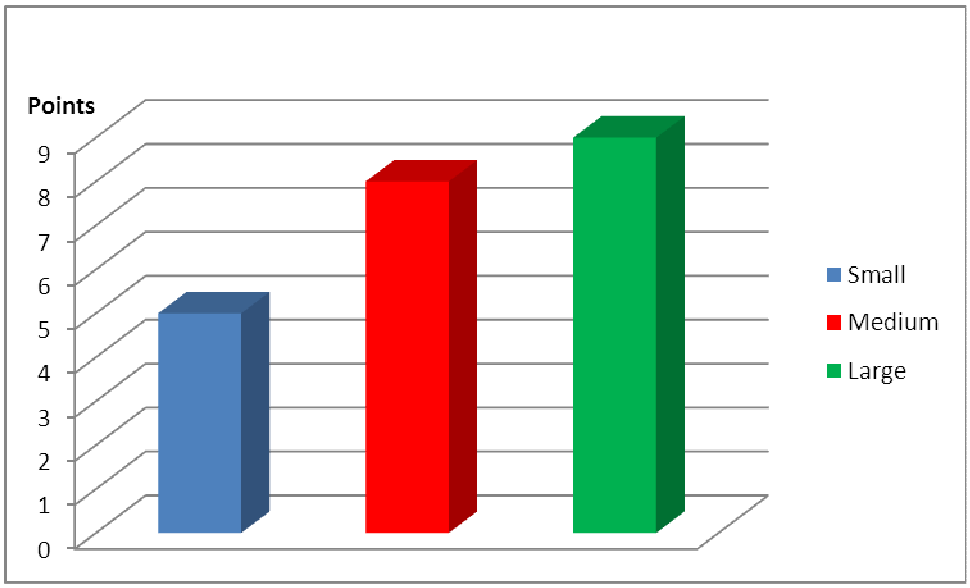
Source: Authors' source

8. I change my password at least once per 45 days



Source: Authors' source

9. I was cognizant of the facts of data security and other issues before signing a contract of employment or during the training



Source: Authors' source

8.2 Supplement 2

Dotazník

Tento dotazník je vytvořen za účelem shromáždění podkladů pro výzkum v diplomové práci týkající se zabezpečení dat.
*Povinné pole

1) Pro přihlášení do operačního systému počítače používám heslo *
- (•) ANO
- ( ) NE

2) Pro přihlášení do podnikových aplikací a jiných internetových aplikací používám heslo/hesla *
- ( ) ANO
- ( ) NE

3) Počet znaků mého nejkratšího hesla *
- ( ) Méně než 8 znaků
- ( ) 8 a více znaků

4) Pro zapamatování hesla jsem použil minimálně jednu z možností (zaškrtněte ano, pokud se i částečně shodujete s jedním z těchto případů): jméno, příjmení, jméno člena rodiny či domácího mazlíčka, přezdívku, rodné číslo, pravidelnou posloupnost čísel, stejný znak *
- ( ) ANO
- ( ) NE

5) Mé nejkratší heslo obsahuje: (napište číslicemi: počet číslic, počet písmen velkých, počet písmen malých, počet jiných znaků) *
*Příklad: SanFrancisco2000** bude zadáno ve tvaru 4,2,10,2*

6) Své heslo jsem sdělil druhé osobě *
- ( ) ANO
- ( ) NE

7) Své heslo mám zapsáno v blízkosti počítače *
- ( ) ANO
- ( ) NE

8) Své heslo měním minimálně jednou za 45 dní *
- ( ) ANO
- ( ) NE

9) O zabezpečení dat a podobné problematice jsem byl poučen v pracovní smlouvě či při školení *
- ( ) ANO
- ( ) NE

Děkuji za vyplnění dotazníku.

Odeslat