Current Trends in Technology and Science
ISSN: 2279- 0535. Volume: 3, Issue: 4(June-July 2014)

Information Security and Personal Data Protection

Silvia Klincekova
Designation : Student *, Organization : University of Ss. Cyril and Methodius in Trnava, Faculty of Mass Media Communication*, Email ID* : silvia.klincekova@gmail.com

Abstract — The paper deals with the issue of information security and protection of personal data. It also describes particular elements of information security which are: assets, threats, vulnerability, impact, risk and restrictions. The important role plays the information security in the company. This started to be the current discussed topic. It can be divided into the three strategies such as: business impact analysis, data classification and risk assessment. The paper contains overview about the personal data policy and new term called pseudonymous data. The companies started to realize that it is a crucial to protect personal data of the customers. It is an essential to protect it more than ever before.

Keywords – information, information security, personal data, protection. pseudonymous data.

1. Introduction

Today's post modern society depends on the information which is processed by using of modern information and communication technologies. It means that the central principles are related on confidentiality, integrity and availability of information and resources. Information security and privacy of personal data have gained an important role. It has become one of the current topic which need to be highlighted.

Information security has been constantly evolving. We are witnesses that some companies do not pay sufficient attention to the information security. It can be affected by the fact of unqualified employees or insufficiency financial sources. Information security is defined as a protection of any kind of information during the whole life cycle, i.e. from their creation to their disposal. The main objective of information security is to ensure the confidentiality, integrity and availability. One of the key challenges in information security are the ability to strike a balance between tactical requirements, respond to changes, keep operational activities and elevate the role of information security in order to become a part of the corporate strategy and as well as decision-making process.

2. The Role of Information and Information Security

If the term information security divided into the subcategory such as information then it could be considered as an asset. This asset can be anything what has own value for particular company. Information is the main asset for the organization. They are necessary for the operation and proper function of the organization.

Protection of information must be secured by:

- only authorized people have access to them
- processing only genuine information,
- possibility to find out who created, changed and deleted the information,
- make sure that the information is not disclosed in an uncontrolled manner,
- availability of information when it is needed.

2.1 The elements of information security

Assets

It can include: process of information and data, creation of products and company image. These mentioned assets are important for company and its business, therefore they must to be protected. At first, companies need to identify which assets must be protected and according to this sufficient information security should be created. It will depend on particular company whether they will pay more or less attention to protect their assets. The business environment needs to be taken under the consideration. [1]

Threats

Threat can be considered as an unpleasant phenomenon which may damage the system or even the organization. It means that the threat may cause an undesirable incident or it can be also defined as an attack on the information.

Vulnerability

It is a weak point inside the company which can be a threat and it can cause some errors or damages to the company. It can be in the area of physical, organizational, personnel, management and administration or information. The causes of vulnerabilities can be:

- high consistency of information,
- the complexity of the software,
- errors in implementation.

Impact

The impact is a result of threats and incidents that have happened. Its consequences can be in the form of loss of information or damage to the assets of the system. The other examples may be financial loss or loss of reputation and good image.

Risk

It represents a risk for the company such as using the new methods in information security, which may arise various problems. Company needs to decide if this change will be realized or they will try to avoid the risks. Alternatively they can choose different methods which will present lower risk.

Restrictions

It represents own measures to enhance the protection of information security. The important role has also the environment where the companies run their business activities. Any kinds of change must be identified for existing and new restrictions. These restrictions can be changed over the time or it can be influenced by the development of the company.

Information security can be achieved by introducing various security measures which are necessary to implement, monitor, review and improve. These individual measures should be implemented in collaboration with other managerial processes inside of company.

3. INFORMATION SECURITY IN COMPANY

Most of companies are aware of the key role of information, but only small percentage of them act according to this. The cause of benevolent approach to safety is especially misjudgment risk of theft and misuse of databases with sensitive data. According to the safety there is an unwillingness of companies to inform about the attacks on their own database of their clients. Any kind of information is taboo, because company does not want to lose or even risk trustworthiness and loyalty of their customers. The reason why company invests into the various security technologies such as: firewalls, intrusion detection systems, antivirus systems, identity management, security incident management etc. is eventually ensure the availability, integrity and confidentiality of the information society. Security is one of the conditions for successful business on the market. The solutions for these fundamental issues could be carried out the evaluation of the safety status of the company i.e. launching analysis of information security projects, such as the analysis of functional range (Business Impact Analysis), data classification (Classification Data) and risk analysis (Risk Assessment).

Business Impact Analysis

The output of BIA is an independent report without any subjective effects on business results taken with respect to the risks associated with any applicable threats to business. BIA is a management of proper setting priorities for information security in the company. It is also the basis for implementing BCM (Business Continuity Management) plan of further development of information security projects, which builds on the results of the BIA.

Data Classification

It is detailed analysis of the company's assets which is focused on critical assets and their classification with considering the state, the sensitivity and value of their content. Data classification leads to the definition of the protection profile, thus to ensure the efficiency of selection of the proper security measures to protect data against loss, unauthorized modification and avoidance.

Risk Assessment

It is important to identify and compliance with the management what are the specific probabilities or chances that identified threats will be carried out and thus affect the business goals of the company. It is the basis for security policy and functionally activate safety management in company.

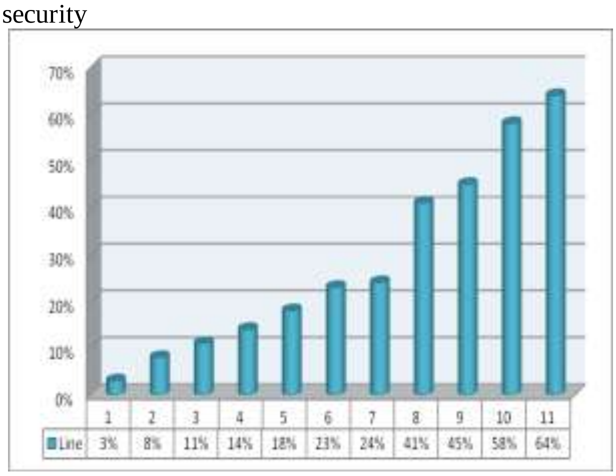
4. Policy of PERSONAL DATA

Protection of privacy and personal data have become a central issue, especially because of its focus on the consumer. Stories in media about the breaches of the privacy, identity theft and the loss of personal data, these not only escalated awareness of consumers, but it also encourages a sense of personal responsibility of executives and the absolute need to bring the protection of privacy and personal data to the forefront.

According to DPA (Data Protection Act) we can defined **Personal Data** as: *“data which relate to a living individual who can be identified from those data, or from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.”* [2]

More and more companies started to pay higher attention to the consequences of loss or theft of customer data. From the global research of Ernst & Young company about information security we can highlighted that 58% identified privacy and data protection as one of the three most powerful driving forces in enterprise policy, while 73% of CEOs and 64% of IT directors gave great emphasis on the importance of privacy and data assets. The results can be seen in the chart below. [3]

Chart no.1: Factors which influence information security



Legend: 1) Risk management in relation to the suppliers, 2) Risk to the business partners, 3) Requirements of information security certifications, 4) New Technologies, 5) The risk in relation with the customers, 6) Phishing, spyware and other technological threats, 7) Impairment of business name/ reputation, 8) Risk management, 9) The achievement of business goals, 10) Data protection and personal data, 11) Compliance with legislation

We can consider that the access to our users, customers or target audience is more important than ever before. We have to take under the consideration also the current fragmented situation of the media. Many professionals agree that data about their users have gained new meaning and perspective. During the day we visit many websites and according to this fact marketers can find out valuable information about us. That is why we will need clear rules of data protection which will protect the customers and marketers will be able to receive needed data. The solution of this discussed topic can be new term – **pseudonymous data**. It is a data which does not say anything about the privacy of the users, but on the other hand they are not absolutely impersonal. It is a data which we can not assign to a particular person but it has certain value for marketers. They are able to use them more precisely and individual. The example of this kind of data can be the information which says who visit our website or who is thinking about buying a new car through the website which she/he has visited previously. Marketers can use this data to gain the target audience in a right time and place. The term pseudonymous data has been unknown until now. It is important that the legislation revaluate the definition of personal data. It is crucial that regulator will understand the market and marketers as well understand the role of data in marketing. New dividing of data (personal, general and pseudonymous) can help marketers to satisfy consumers and which information is used about them. We make sure that the personal data of our consumers will be accessed to the highest level of protection.

Business enterprise subject which prove the experience of implementing and ensuring strong protection to carry out checks in compliance with the safety of the practice can develop these attributes in their business and thereby positively distinguish from competitors, increase market share, improve the reputation and increase profits.

ACKNOWLEDGEMENT

This paper is one of the outputs of a research for project **VEGA no. 1/0558/12** *„Research on the factors of affecting the selection and implementation of integrated marketing communication with regard to the safety and protection of customers.“*

REFERENCES

[1] Ondrej Strnad, Bezpecnosť a manazment ifnormacnych systemov. Bratislava: STU, 2009. p. 344. ISBN 978-80-227-3040-2.
[2] Definition of personal data and sensitive personal data, [online]. Available from: http://www.yourrights.org.uk/yourrights/privacy/data-protection/definition-of-personal-data.shtml [21.06.2014].
[3] Lukas Neduchal, Informacna bezpecnosť – dosiahnutie rovnováhy medzi rizikom a vykonnosťou, Vol. 2., p. 13 – 16, 2008.
[4] MediaCom, Pseudonymné data – nove riesenie ochrany osobných údajov, Stratégie, Vol. 11., p. 15, 2013.

AUTHOR'S PROFILE

Mgr. Silvia Klincekova is an external PhD student at University of Ss. Cyril and Methodius in Trnava, Faculty of Mass Media Communication. The dissertation thesis is: The Attributes of customer value in the context of the global market.