UDC 004.041:005.92

LEAKING OF CONFIDENTIAL PERSONAL INFORMATION

Marjan Marjanovic

Security Guard Montenegro, Podgorica, Montenegro, marjan@securityguardmn.com

Abstract: *The aim of this paper is to point to the significance of corporate information security and empirical study of leaking confidential personal information in 2017 in the world, for commercial and non-commercial state organizations, which were caused by malicious or neglecting activities of employees or external attackers and their percentage share according to the criteria determined. The study was based on database created based on public announcement on the cases of leaking of confidential information. The criteria includes less than 1% of cases of the assumed total number of leaking. The criteria of this categorization of leaking were chosen in such a manner that category studying contains enough elements in order for the research field formation to enable the theoretical observation of the sample and the results and trends observed the generalization of the conclusion. The results have shown that in 2017 there were registered 1505 cases of information leaking, of which 965,9 million of personal. 32,2% was caused by external ill-wisher and 65,4% the employees. Personal data and financial information are the most frequent objects of the attack – 90,8%. The networks are the most frequent channels of leaking information– 45,6%. The greatest percentage of information leaking is in commercial medium companies and the most attractive economy branch for the attacks is in the field of high technologies, trade and transport. The data of trade, transport and high technology organizations are usually attacked from the outside, while financial, medical and educational organizations are as a rule attacked by the insiders. For the theft of the data, less and less are used electronic mail, portable media, services for rapid messages because the control of these channels is big. The sources of hackers are closed uncontrolled channels whose protection systems either do not work or they are not efficient.*

Keywords: *corporate security, information protection, information security, leaking of confidential personal information.*

1. INTRODUCTION

Information protection, i.e. information security, is the subject of a general interest of both state institutions and corporations and other economy subjects. In that aspect, as one of the most important tasks, there is defined the development and implementation of reliable methods and means of information protection, as well as looking for systemic solution and means of protection by the application of the most effective algorithms and methods

of projecting means of information protection – information security instruments (Trivan, 2012). Historically, observed, information protection (information security) is defined as: protection of information systems against unauthorized access or modification of information both in warehousing, processing or transfer and against deprieving the authorized users from services, including the required measures of detection, documenting and elimination of such threats. (National Information Systems Security Glossary, 2000) .

For the field of information protection, it is very significant to overcome the arrogance and conservatism that can exist in the part of corporative management, and which can be expressed in underestimating the threats for the integrity of information system, unfamiliarity with basic structure of IS, as well as avoiding communication with the staff who work on jobs of protecting that system. As explanations and excuses for not investing in protection measure, very often there are mentioned their high price and ineffectiveness in the short run. (Rodic, Djordjevic, 2004)

2. DEFINITION AND HISTORICAL DEVELOPMENT OF INFORMATION PROTECTION

Historically observed, information protection is defined as: protection of information systems against unauthorized access or modifications of information both in warehousing, processing or transfer and against service deprivation of authorized users, including the required measures of detection, documentation and elimination of such threats. (National Information Systems Security Glossary, 2000).

As Wolf stresses, historically observed, development of information security has begun in 1960's through COMSEC – Communication Security (Wolf, 2003). With the appearance of the first computers, in the beginning of 1970's, there originated computer security COMSEC and COMPUSEC are joined in information security (INFOSEC - Information Security), which attempted to integrate previously separated disciplines such as security of the personnel, computer security, communication security and operative security.

3. HARMFUL IMPACTS ON INFORMATION INFRASTRUCTURE

Information infrastructure can be exposed to harmful effects of different nature that can directly or indirectly jeopardize its functioning. Those impacts can be classified into failures, incidents and attacks (Ellison et all. 1997). Failures are potentially harmful events, caused by internal defects of the system or defects on external elements required for its functioning. They can be the consequence of mistakes in software designing, as well as consequence of failures of hardware, human mistakes, etc. category of the incidents includes all random events such as natural disasters and catastrophes. Unlike the failures, incidents are the events whose cause is out of the system (Petkovic, 2009).

Attacks on information systems can be defined as direct actions against networks or information systems with the aim to interrupt operations without authorization, take over the control and destroy, change of corrupt their data (memorized or in processing) (Stallings, 1995). According to some authors, we can distinguish three types of attacks on information systems:

- physical attack (Marlin, Darvey, 2004);
- electronic attack;
- cyber attack (Petkovic, 2009).

According to Robert Eagan, among the security threats to the information systems that are of internal origin, the most widely present are material damages, impairments and dysfunctions that occur accidentally, due to reluctance and negligence of the employees, responsible people and managers (Eagan, 2005). External endangerment of information systems can also be different, from the property, through political to computer and other forms of high-tech crime.

Rodic and Djordjevic point out that the attackers are the starting point of each attack to the computer system, although they are different by what they are and where they come from, according to their abilities and whether they are within our outside of the system they are attacking (Rodic, Djordjevic, 2004). In that aspect, the attackers can be divided into six categories: hackers, terrorists, organized attackers, professional criminals (Rodic, Djordjevic, 2004).

Javorovic points out that there are following sources and types of dangers for the information systems of corporations:

- program (software) sources of vulnerability,
- hacker attacks, with the intention of breaking into the information,
- piracy, i.e. illegal multiplication and selling of piracy software,
- physical attacks on information and communication systems, including internal and external thefts of data and information, theft of information equipment, disabling of server, destruction of information equipment, deliberate causing of fire and terrorist attacks to the information systems,
- endangering from the environment,
- internal organizational problems,
- information and business espionage,
- inexcusable and criminal behavior of the users of information systems and networks, especially the Internet,
- technical mistakes in components of information and communication technology (Javorovic, Bilandzic, 2007).

4. METHODS AND MEANS OF INFORMATION PROTECTION

By the measures of information security we imply general rules of data protection that are realized on physical, technical and organizational level. Standards of information security are organizational and technical procedures and solutions meant for systematic and unified implementation of the prescribed measures of information protection (Trivan, 2012). Measures and standards of information security determine minimum criteria for the protection of confidential data in business subjects (Ivandic et al. 2011).

The most significant international norm for management of information security is the standard ISO/IEC 27001:2005, which defines requests for establishment, maintenance and continuous improvement of information security management system. Specificity of this norm is in the fact that the term of information secuirty is not observed exclusively from

information aspect, but also predicts the application of other elements of corporate security, such as physical and technical security, human resources management, legal protects, etc.

The norm ISO 27001 contains the guidelines and specifications for the help to the organizations that are developing ISMS – Information Security Management System. ISMS is a systematic approach to the security management of information that are in the possession of an organization, and it includes executors, processes, information systems, policies and procedures (Ivandic et al. 2011).

According to B. Javorovic, in order to protect the information systems, corporation should implement the measures that include different areas: normative-legal measures, primarily the adoption of the Rulebook on information and communication protection, by which we could develop the rights, obligations and responsibilities of all the structures in the company, from the management and organizational units up to each employee; organizational measures, including system establishment (organizational units) for information and communication security, organizational solutions for implementation of particular protection measures (access level to information bases, procedures and actions, network security, organization of security zones, etc.); program measures (timely programming of appropriate protection procedures according to the questions: who? what? of which? where? when? how? by what? And the like, the application of the anti-virus protection program, protection against the hackers and other types of external endangering, setting the so-called firewall protection, the application of «strong» passwords, program update, etc.); technical and technological measures (usage of protection possibilities of the very information and communication technology, application of technical means in that protection, including alarm systems, video surveillance, systems for limiting the access to the premises, servers and bases and the like); personnel measures (security procedures in the selection of business, management and leading professional staff and reception of new employees, nomination of information management, selection of capable system and network administrators, etc.); education measures (security training of all employees and different forms of professional improvement in implementation of security procedures and protection measures, acquisition of appropriate certificates and the like); supervision, which includes the tours of restrictive space, review of the software and hardware, testing, monitoring of activities and security incidents, permanent communication with responsible management and professional staff, an insight into the application of international and national regulations and norms, etc.); sanctions, which depending on the seriousness of the inflicted damage can range from the hearing, warning, reduction of salary, compensation for the damage, change of the workplace, abolishment of authorization, up to the firing and prosecution; physical measures that include that supervision of entrance-exit places, identification of visitors and their leading to the destination, prevention of unauthorized entrance and movement in the business premises, prevention of burglaries and thefts, interventions in case of a fire and other accidents and the like; counter-inteligence measures, which are taken at software, hardware, technical and physical level, with the aim to prevent illegal, unauthorized penetration into secret databases, which can be attempted by competition (national and international) corporations or foreign intelligence services; security regulation of business environment (measures for the maintenance of optimal temperature and reduction of moisture, noise, dust), in order to protect and provide secure work of information and communication systems (Javorovic, Bilandzic, 2007).

5. PREVENTION OF UNAUTHORIZED ACCESS TO INFORMATION SYSTEMS OF CORPORATIONS

Some authors point out that the protection of corporations' information systems against unauthorized access includes four areas significant for information security: security verification, physical security, data security and information system security (Ivandic et al. 2011).

By the authorization, the user is even after the access to the information system limited in actions and manipulations with data and information. In that aspect, each implemented action on data and/or information should be registered, especially if they have occurred (Rodic, Djordjevic, 2004).

6. AUTHENTICATION AND NON-REPUDIATION OF INFORMATION

The progress in computer technique and appearance of networks (LAN and WAN and, first of all, INTERNET), has extended the list of information properties, before which there are some security requirements set. Those are primarily authentication and non-repudiation. Based on the mentioned features of information, ther concept of information security was defined in the 1990's. It is important to observe that the difference is not only of a terminological nature, but it is also about essential changes (Stephenson, 2010).

Determination of authentication means proving that the user of information system is really the person that it is said to be. Such a proof usually consists of the combination of data on the following characteristics of users: something that only one person knows (password), something that only one person has (card), something that only one person is (fingerprint), something that undoubtedly represents the behavior of a person (handwriting, speech). Verification of authenticity is the ability of the system to verify the identifier (or several of them) that are pointed out by the user, i.e. determines whether the system is accessed by the user whose identifier is pointed to the system (Rodic, Djordjevic, 2004).

7. DETECTION AND REACTION

Important characteristics of information security and operativity (operational in nature) and sensitivity to time (time-sensitive). There characteristics are expressed by the terms detection and reaction. It is about defansive operational possibilities for which, along with traditional information and protection activities, from the late 1990's, we use terms of information war theory, i.e. Defensive Information Operations – DIO (Field Manual, 2010). The term information security in the USA was officially introduced in 2002, by the directive of the Ministry of Defense. According to that document, information security (IS) consists of "information operations of protection and defense of information and information systems, which enable their disposability, integrity, authenticity, confidentiality and non-repudation and it implies the restauration of information systems by incorporated possibilities of protection, detection and reaction" (Department of Defense Directive No. 8500.1, 2002).

8. COMPARATIVE PRACTICE OF INFORMATION PROTECTION IN THE MOST SIGNIFICANT CONTEMPORARY MODERN

According to Zdravko Bazdan, information systems of corporations can be divided into: information systems for collection and processing of data; information systems (internal informing of managers and employees, informing of business partners and the like); information systems, which are the base for all information and business structures; integral information systems, which consist of data and information sources, their collection, selection, verification through data processing, information processing, creation, development and maintenance of information bases, presentations of certain segments or whole collected information material, transfer to the user, monitoring of success and efficiency of system's work, then return of information through entering the results in own base of data and information, with the optimal supervision and management. The main part of that system – information operative unit, often called Operative-Information Center (OIC). At the top of information system within the corporation there is management or information management, which has subordinate services for development and construction of information system, study of information needs, user processing and preparation of information, business-intelligence activity and for information supervision and security issues. According to Z. Bezdan's data, among the modern transnational and multinational corporations, the most complex information systems have General Electric, Royal Dutch Shell, General Motors, Toyota Motors, Exxon Mobil, British Petroleum (BP) and JP Morgan Chase, which are also according to other parameters among the most powerful companies in the world (Bezdan, 2009).

As it is stressed by B. Rodic and G. Djordjevic, some threats to information systems of corporations remain unrevealed, due to which special services are engaged to discover or evaluate the possibility of a threat. At the same time, vulnerability of the system is vice versa to the level of its defense. The significance of the very information system depends on its financial, material or political value. The analysis of threats, vulnerability and significance of the system, availability of counter-measures and ration of risk price and cost price helps in leading and determining the required activities of company's management and priorities in the work with risks in protection of information, as well as in case of introducing controls of the nominated in order to protect against those risks. In some situations, it is required to stress that the process of evaluating the risk and selection of control are repeated a few time in order to include different parts of corporation or individual information systems. Methods of risk evaluation can be applied to the whole organization, or only some its parts, as well as individual information systems, specific components of the system or services, as well as the functions, in cases where it is feasible and where it is of help (Rodic, Djordjevic, 2004).

Bozidar Javorovic points that information systems have become to the world what the nervous system and bloodstream are for the human organism, so that the crush of the global information system would lead to the drop of modern civilization and return the living man to the level from the distant past. At the microlevel of corporation, destroying the database or internal information system would imply business capastrophe that many companies would not survive. According to this author, the problem is that with greater complexity, size and importance of information systems, their sensitivity to all types of attacks and en-

dangerments that the consequences of its destruction become harder and harder (Javorovic, Bilandzic, 2007).

Modern global corporations believe that information security is one of the most important priorities in leading their business. In accordance with that, radical changes in organization of information security service in those companies are obvious, they are not only separated from the service for development and application of information technologies, but very often there are introduced the functions of directors (CISI) and managers of information security (BISO). This shows that the issues of information security and issues of business information protection, which were recently considered marginal, have come to the position to be the scope of interest of the very top management (Muravjeva, 2006).

9. EMPIRICAL STUDY OF LEAKING THE CONFIDENTIAL INFORMATION IN THE WORLD METHODOLOGY

In recent couple of years from cover pages and striking news of the leading media houses we were continuously informed on the leaking of confidential information of global corporations. It is about big and significant names of corporations, victims of the theft of confidential information: Anthem, Apple, AT&T, British Airways, DreamWorks, Electronic Arts, Equifax, FIA, Google, HBO, HSBC, HTC, JP Morgan Chase, Kia Motors, Lenovo, Lufthanse, Microsoft, Morgan Stanley, NVIDIS, PayPal, PwC, Samsung, Starbucks, Tele2, Toyota, Twitter, Uber, United Airlines, Yahoo.

In 2016., in the world there were registered 1395 cases of leaking of confidential information, which is 22% more than 2015. (source: http://bis-expert.ru/bis-summit). The most leaking was connected with personal data – 92%. More than 767 millions of personal data were compromised due to the errors of intentional activities of internal attackers. In 2016., there was recorded 14 big cases – there leaked more than 10 million of personal data, which is 89% of all compromised recordings. Banks, Internet services and medical institutions were the most frequent targets of the attack. In 55% cases, the culprits of the leaking of confidential information were the employees in companies and in one case it was a highly positioned manager of the organization (source: http://bis-expert.ru/bis-summit). Eleven and a half million of documents have leaked from one of the main agencies for the establishment of off-shore companies „„Mossack Fonseca"". The papers reveal the names of different politicians, criminals, businessmen and celebrities who have been hiding behind the companies founded in tax paradises. In this study, led by ICIJ and "Suddeutsche Zeitung" there have participated more than 100 editorial staff teams throughout the world (source: https://www.krik.rs/najvece-curenje-informacija-iz-ofsor-zona-u-istoriji/#sthash.X1CstAty.dpuf).

Due to everything above mentioned, the subject of the study is the leaking of confidential personal information.

In this paper, there are combined qualitative and quantitative methodological approach, the so-called triangulation method. Techniques and instruments were chosen within descriptive research method. There were applied the analytical-synthetical and statistical method, as well as content analysis.

Research was based on a database created based on public announcements on the cases of leaking of confidential information (means of a public informing, blogs, Internet forums,

other open sources) from commercial and non-commercial state organizations, to which it came by malicious or negligent actions of employees or external attackers.

In case of creating the base, each leaking of data was classified according to the following criteria: size of organization, industry branch, damage level, type of leakage (according to the intention), leaking channel, type of information.

Sample

The study includes less than 1% of case of the supposed total number of leaking. However, the criteria of leaking categorization are chosen so that the study if many categories contains sufficient elements in order for the formation of research field to enable the theoretical observation of the sample and the results of the study and the trends observed the generalization of the conclusion.

In order for the sample to be as harmonized as possible, from the study we have excluded the so-called "mega leaking" (more than 10 million of information) of personal information, as well as those with less than 100.

Cases of impairing the confidentiality of information and similar incidents that did not result in leaking of information, as well as those with the unclear data source (when we do not know which organization had the information) were not included in research sample.

It is important to mention the fact that these incidents are only the top of the iceberg. In 2017., there were many cases of confidential information leaking recorded from medical and financial institutions, most frequent due to the error or carelessness of the employees.

The goal of the study is to determine the number of leakages of confidential personal information in 2017 in the world, based on public announcements on cases of leakage of confidential information (public information means, blogs, Internet forums, other open sources) from commercial and non-commercial state organizations, to which it came by malicious and negligent activities of employees or external attackers and their percentage share by different criteria: size of an organization, industry branch, damage level, leakage type (according to the intention), leakage channel, information type.

Based on the subject and goal of the study, the following **tasks** were set:

1. study public announcements on leakage of confidential information in the world.
2. create a database based on the studies of announcements of confidential information leakage cases in the world.
3. classify leakage of data according to the following criteria: size of an organization, industry branch, damage level, leakage type (according to the intention), leakage channel, information type.
4. set aside the spotted trends.

Hypotheses

H0 leakage of confidential information is rising

H1 internal attacks are the most frequent types of activities

H2 the employees are the most frequent information leakage type

H3 personal data and financial information are the most frequent objects of the attack.

H4 networks are the most frequent channels of information leakage in cases of random information leakage

H5 networks are the most frequent information leakage channels in cases of intentional

information leakage
H6 medium enterprises are most frequently the targets of the attack to confidential personal information
H7 the greatest percentage of information leakage is in commercial enterprises
H8 the most attractive industry branch for the attacks is in the field of high technologies, trade and transport.

10. RESULTS OF THE STUDY WITH DISCUSSION

In 2017., there were registered 1505 cases of confidential information leakage, of which 965,9 million were personal – numbers of social insurance, bank cards and other confidential and important information.

Table 1. Leakage of information by activity vector

No.	Activity vector	Percentage
1.	External attacks	32,2
2.	Internal attacks	64,4
3.	Unclassified	2,5

There were registered 484 or 32,2% information leakages whose cause is the external ill-wisher. In 984 or 65,4% cases, the leakage of confidential information occurred due to the guilt of employees. External attacks were recorded in 15 out of 21 cases of mega leakage.

By this, we have proven our H1 hypothesis **Internal attacks are the most frequent type of activity.**

Confidential information leakage caused by external attacks is characterized by a greater range of compromised data. On the average, per one external attack there are compromised about 1,26 million data, while in case of the internal attack, it is 0,34 million. This, of course, does not imply that leakage that came from the inside is less devastating and dangerous than the one that occurred due to the external attack.

Table 2. Information leakage according to the source

No.	Leakage source	Percentage
1.	Manager	1,1
2.	System administrator	1,4
3.	Employees	48,9
4.	Former employees	2,3
5.	External associate	7,6
6.	External ill-wisher	32,2
7.	Unclassified	6,5

As it is presented in Table 2. in 2017. in 51,2% cases the culprits for information leakage were current or former employees (48,9% and 2,3%). In more than 1% of cases, there was recorded the culprit of organization's managers (top management, department management and the like), which confirms our hypothesis **H2 the employees are the most frequent information leakage type.** There is a very high percentage of leakage that occurred by external associates who have the access to the protected information, 3,5%.

Table 3. Information leakage according to the data type

No.	Data type	Percentage
1.	Personal data and financial information	90,8%
2.	Commercial secret, know-how	5%
3.	State secret	1,7
4.	Unclassified	2,5

The highest percentage of confidential information leakage is in the domain of personal and financial data – 90,8%, then there are commercial with 5%, state secret with 1,7% and 2,5% are unclassified, which confirms our third auxiliary hypothesis **H3 personal data and financial information are the most frequent objects of the attack.**

Table 4. Incidents by the character

No.	Character of the incidents	Percentage
1.	Information leakage	82
2.	Fraud by using the data	10,3
3.	Overrun of right to access information	7,7

The thing that we have observed as a main trend on a global sample of our study is a high level of information leakage caused by malicious attacks from the outside. Almost 2/3 of the compromised personal information in 2017. occurred as a result of external attacks. There are set aside the incidents that refer to illegal activities of the hackers, penetration into infrastructure of the company, theft of information on clients and employees.

Channels of information leakage

In 2017., most frequently registered information leakage channels were: the loss of equipment, electronic mail, paper documents, as well as portable media, mobile devices, text of the video message and social networks. Comparing the data obtained in our study to the data from 2016, we observe the trend of information leakage reduction due to the loss of equipment, electronic mail and paper documents. Another trend is observable when we look at information leakage channels. Namely a great number of cases where we cannot precisely determine the leakage channels and percentage of such information loss is 21,3%.

Table 5. Information leakage channels

No.	Information leakage channels	Percentage
1.	theft/equipment loss	7,6
2.	Mobile devices	0,2
3.	Portable media	3,6
4.	network (browser, cloud...)	45,6
5.	Electronic mail	7,5
6.	Paper documents	14
7.	Video materials	0,3
8.	Unclassified	21,3

There is an opinion that cases of random information leakage are less harmful for the company than ill-wishers. However, this is a wrong assumption. The practice has shown that the consequences do not depend on the type of leakage or the sources of activity than the character of the information lost.

Table 6. Random and intentional information leakage cases

No.	Information leakage channel	Percentage	
		Random	Intentional
1.	Theft/equipment loss	1,5	0,4
2.	Mobile devices	0,3	0,2
3.	Portable media	5,5	0,4
4.	Network (browser, cloud...)	27,4	73
5.	Electronic mail	12,1	2,1
6.	Paper documents	21,9	2,1
7.	Video materials	10,3	0,1
8.	Unclassified	21	21,7

It is important to mention that the networks are the most critical information leakage channels and both in case of random and intentional. This confirms our hypotheses **H4 Networks are the most frequent channels of information leakage in case of random information leakage and H5 Networks are the most frequent information leakage channels in case of intentional information leakage.** Network information leakage is characterized by a high level of data criticality and a big scope of compromising information. As a result of external attacks there appears a great financial loss for the company. Only one incident can drastically change the future of the company and have a negative effect on its strategy.

45% network incidents refer to financial data – numbers of accounts, balances, credit cards.

Table 7. Financial data leakage by channels

No.	Information leakage channel	Percentage
1.	Theft/equipment loss	7,57
2.	Portable devices	0,63
3.	Portable media	3,56
4.	Network (browser, cloud…)	45,57%
5.	Electronic mail	7,49
6.	Paper documents	14%
7.	Video materials	0
8.	Unclassified	21,27

Small percentage of intentional information leakage through mobile devices, portable media, electronic mail and paper documents can be explained by the fact that those channels are less and less used for malicious attacks. The attackers are aware that through modern means of control we can successfully intersect the transfers of confidential information through these channels and for that reason they do not risk failure.

Domination of network channels both in case of intentional and unintentional information leakage testifies, primarily, on the growing significance of this channels to business. Number of communication services connected to the network is very big. The amount of employees' mistakes who work in those services is growing year after year. Accordingly, there also grows the number of random information leakage in case of information spreading through the network, publishing of data on the Web and so on.

On the other hand, ill-wishers more and more rarely use these channels in which there is controlled information transfer – electronic mail, rapid announcements services and the like.

Confidential information leakage according to the type of the company.

According to the type of organizations, the highest percentage of information leakage occurs in commercial – 72,8%, then state– 17%, and 10,2% is unclassified which confirms our seventh additional hypothesis **H7 the greatest percentage of information leakage is in commercial companies.**

If we however look at industry branches, we will observe that the greatest percentage is in trade – 63,9%, then in high tech branches (Internet services, selling websites and the like) – 63,2%, then there follows the production and transport with 61,6%, banks and finances with 51,3%, then medicine – 26,1%, oil and gas – 25,9%, education 24%, public and state government 7,8%, which confirms our eight additional hypothesis **H8 the most attractive industry branch for the attacks was in the field of high technologies, trade and transport.**

The attraction of industry branch for the attacks is conditioned by the data liquidity that the company owns. The assumption of the attacker on the data protection level in the industry branch also affects the attractiveness, but vice versa. The attraction of the branch finds the ultimate confirmation in the number of recorded intentional information leakage.

One of the main reasons of the high percentage of information theft in medical and financial institutions is a low level of the culture of using the information of a limited access and high liquidity of data.

According to the size of the company there also exists the difference. The greatest percentage of information leakage was recorded in medium companies – 85%, then big – 8,7% and the least in small – 6,3%. Thus we confirm ours hypothesis **HG Medium companies are the most frequent targets of the attack to confidential information.**

It is important to mention that such a situation has appeared two to three years back and primarily in medical and trade companies.

We can conclude that for the intentional attacks, the most attractive are the industry branches: parts of high technology, trade, transport. The greatest range if compromising data, without mega-leakage, was observed in high-tech companies and in educational institutions. Trade, transport and high-tech companies most frequently attack from the outside and the banks, medicine and insurance companies with the help of employees. Medium business was subject to personal data leakage in a much greater level than big business.

11. CONCLUSION

When you type in the browser the keywords "confidential data leakage" within a few seconds there appears about 2,860 results, which only testifies on the size of the problem that this paper deals with.

After the introductory remarks, the paper defines information protection and provides its historical development, with an insight to the most recent authors dealing with these issues in our country and abroad. Then, in this paper we also talk about harmful effect and information infrastructure (failure, incidents and attacks), and thus there are mentioned possible methods and means of information protection.

The last part of the theoretical consideration in this paper was dedicated to comparative practice of information protection in the most significant modern corporations.

Discovery of sensitive business data can have serious consequences for the business of one company, its reputation or even survival.

For an adequate access to solving this issue, it is required to understand its causes, whether they are technical or they belong to the human nature and behavior.

The consequences of data losses can be direct or indirect. Direct consequences can be observed in a specific financial manner. They occur after the loss of personal and financial data of the clients. Indirect consequences are more easier to observe because they appear during a longer period of time and their financial weight cannot always be precisely determined. These consequences occur after the loss of critical business data and intellectual property and they cause the impairing of the company's reputation, turning of clients to more competitive companies and reduction of business scope.

Prevention of data leakage should be aimed towards the most risky aspects of business practice.

Empirical part of the paper deals with the most significant incidents in 2017 in relation to the illegal activities of hackers, penetration in infrastructure of the company, theft of information on employees and clients.

Research has shown that for data theft we less and less use electronic mail, portable media, services of rapid messages, due to the fact that control of these channels is big. The choice of hackers are more and more the closed uncontrolled channels whose protection systems either do not work or they are inefficient.

The most attractive to the attackers are the companies in the field of high technologies, trade and transport. The data of tarde, transport and high-tech organizations are most frequently attacked from the outside, while financial, medical and educational organizations, as a rule attacked by the insiders.

The study has shown that medium companies are most frequently the victims of the personal data leakage than it is the case of the big ones.

The data obtained by the study have confirmed all the hypotheses set.

The theme of data leakage becomes more and more transparent, which is very good and useful. Let's hope that in the future we will talk not only of the leakage, data types, features of the channels, but also the evaluation of protection, real financial losses of specific media due to leakage of a certain type of information, then the incident level.

REFERENCES

Bazdan, Z. (2009). *Menadžeri moraju znati: poslovno obavještajna djelatnost kreira najvažniji resurs upravljanja*, Poslovna izvrsnost, god. III, br. 2, Hrvatski institut za kvalitetu, Zagreb, str. 62.

Ellison R.J., Fisher D.A., Linger R.C., Lipson H.F., Longstaff T., Mead N.R., (1997). *Survivable Network Systems: An Emerging Discipline, Technical Report (CMU/SEI-97-TR-013.ESC-TR-97-013),* CERT, Pittsburgh PA

Field Manual No. 3-13, FM 3-13 (FM 100-6), in: Information operations: Doctrine, Tactics, Techniques and Procedures, Department of the Army, Washington DC, November 2003.

Ivandić Vidović D., Karlović L., Ostojić A. (2011). Korporativna sigurnost, Udruga hrvatskih menadžera sigurnosti – UHMS, Zagreb

Javorović B., Bilandžić M. (2007). Poslovne informacije i biznis inteligence, Golden marketing, Tehnička knjiga, Zagreb

Marlin, S., Darvey M. (2004). *Disaster-Recovery Spending on the Rise*", Information Week, Manhasset NY, Avgust 2004., p. 26.

Муравъева И. (2006). Новый взгляд на службу информационной безопасности компании, (http: www.bre.ru/security/20033.html). доступан 14. 08. 2016.

National Information Systems Security Glossary, NSTISSI No 4009, National Security Agency, Fort Meade MD, September 2000.

Petković, T. (2009). Poslovna špijunaža i ekonomsko ratovanje, Protexi Group System, Novi Sad

Rodić, B., Đorđević G. (2004). Da li ste sigurni da ste bezbedni, Produktivnost, Beograd

Trivan, D. (2012). Korporativna bezbednost, Dosije studio, Beograd

Stallings, W. (1995). *Network and Internetwork Security – Principles and Practice*, Prentice Hall, Englewood Cliffs, New Jersey

Stephenson, P. (2010). *Authentication: A pillar of information assurance*, SC Magazine, Vol. 21, No. 1, New York, January 2010., p. 55.

Wolf G. D. (2003). *Statement before the House Select Committee on Homeland Security Subcommittee on Cybersecurity, Science and Research & Development*, National Security Agency US, Fort Meade MD.

http://bis-expert.ru/bis-summit