Status of the Risks Caused by Information Leaks from Commercial Banks in Bulgaria

Petya Biolcheva*

Summary:

Information is one of the key assets of commercial banks. The loss of bank information in question might cause serious financial and reputational damage to the bank. In the recent years, criminal activities related to bank robberies are occurring ever more often, bringing new risks of the criminogenic nature. Primary position among them occupies cybercrime involving siphoning off bank information. This article is aimed at detecting trends associated with the risk of information leaks. Below are the protection mechanisms and most often risk situations that threaten the banking information security. There is a well outlined trend in respect of the risks of major internal and external sources of threat. An analysis is presented and basic mechanisms for preventing the risk of leaks. Below are the economic and other negative effects on bank security and banks as a whole, in the absence of timely prevention of the risk of leaks.

Key words: commercial banks, bank security, data leaks, bank information, risk prevention

JEL Classification: E580; H55; G29

1. Introduction

Over the last decade, banks have become increasingly reliant on digital information to meet business objectives. On any given business day, significant amounts of information fuel business processes that involve parties both inside and outside of banks network boundaries. (Antony and Melek, 2010)

At commercial banks transactions with huge numbers of downloads are held all the time, saving different amounts of cash. Banks work with arrays of sensitive data concerning clients, business partners, regulators, and shareholders that require a high level of protection of the information related to them. At the same time, banks are attractive target for various information attacks, and sometimes victims of massive data loss and information leaks. That is why adequate information protection is required to minimize the risk of various raids and attacks on the banking information resource. Banking Information security is focused on the storage, processing and transmission of information. It means information protection and protection of its supporting infrastructure from accidental or intentional impacts from natural or artificial origin, which may cause unacceptable damage to the owners or to the users and also to the supporting infrastructure. The main objective of the banking information security is to secure and protect information or to minimize its loss.(Social Dude, infirmacionna sigurnost, 2015.)

The object of study in this paper are commercial banks operating in the country

* Assistant Professor, PhD., University in National and World Economy, Department Industrial Business, email: p.biolcheva@unwe.bg

and more specifically - it is the study of the current state of risk prevention concerning information leaks in banks.

The main purpose is to show the most frequently occurring risks, trends, as well as mechanisms to prevent the risk of info leaks.

The concept of information leak can be defined as intentional or unintentional disclosure of data belonging to an organization out to unauthorized persons.

Due to the topicality of the issue, concerned banks regularly carry out individual studies on the state of that kind of risk. It has been discussed at conferences in the country, for example the Tenth Regional Conference on Information Security and Data Storage, held in Sofia in 2011.

In the study are used different statistical methods. Mainly place takes variation analysis with secondary level and statistical distribution.

2. Methodology of the Study

The concept leaks can be defined as intentional or unintentional disclosure of an organization to unauthorized persons. In order to establish the current state of the risk of info leaks from commercial banks operating in the country, a survey and a series of partial in-depth interviews have been made in some of the big banks. It asked questions related to the internal and external sources of leaks. The aim is to establish their frequency and occurrence the Bulgarian banking practice, the forms they take and the severity of their implications.

Some questions offer possible answers for respondents to choose among. Another part requires that the level of risk is measured using a five-point scale. In this scale 1 marks the assessment of the lowest risk, whereas 5 presents the highest possible risk.

The partially in-depth interviews were conducted in meetings with bank managers dealing with the security in the banks. Along with completing the survey questions they have shared their expert views and opinions on the topics of study.

The sample of surveyed banks covers about 30% of the banking sector (BNB, Raiffeisenbank Bulgaria, Eurobank, Piraeus Bank, First Investment Bank, Central Cooperative Bank, etc.) that are licensed to conduct banking business in the country. Given the delicate nature of the issues and preserving the confidentiality of the information received, the data is summarized for the sample of banks.

The concept leaks can be defined as intentional or unintentional disclosure of an organization out to unauthorized persons. The moment at which the empirical study is conducted is the last quarter of 2015. The period that has been studied comprises three years. Respondents were managers in banking security, to whose portfolio falls information security and are respectively responsible for the prevention of info leaks within their banks. Different statistical methods were used and specifical means of questionnaires and interviews processing.

3. Basic Results of the Study

Commercial banks are still suffering the consequences of the destabilization of the banking system in the summer of 2014. About 40% of banks have suffered financial losses and outflow of customers. For other about 40% of the banks in Bulgaria the effect was positively associated with the influx of new customers and cash flows, and signing of new corporate contracts. For about 13% of the banks this destabilization has led to serious reputational damage. Inevitably, all this has affected the banking security and the information security.

When talking about security in banks, the first association appears to be linked to the risk of bank robberies. About 65% of the security managers state that they believe

in the last three years, this risk is reduced. However, about 75% of them see a threat to the safety of bank assets, the life and health of personnel. Over the past three years, robberies were committed in 14% of the commercial banks. Insiders are involved in almost all these cases. It is estimated that about 55% of the banks employees have been subjected to some kind of impact (bribes courtship, threats, etc.) by malicious individuals. Manifestation of this impact is mainly related to the disclosure of confidential information. At 43% of banks in the last three years bank officials have tried for embezzlement or misuse of bank assets.

Similar is the percentage of bank employees through which banking information has leaked. Apart from officials attempted abuse is observed by banking counterparties. Thesse incluse maintenance companies, external software experts, consultants, suppliers and others.

Another risk group for banking security is the banking staff. Over the past three years at 43% of banks the security managers have had problems with the reliability of the staff. They found attempts to circumvent / violate the provisions of the banking security by the staff of the bank. In order to ensure a high level of bank protection departments have established warm trustful relationships with bank staff in everyday talk and through these talks they have clarified certain circumstances in different events (86% of cases). Another factor determining the reliability of personnel is connected with the motivation. In only 29% the bank employees are defined as highly motivated. At the other extreme - not motivated fall another 14%. (See. Figure 1).

The next risk group analyzed in this article is the technical systems for information security. In 86% of banks, security managers believe that investments in innovation related to information security systems are appropriate. They provide a high level of protection not less than that of the competing banks. At the same time they work in the direction of reducing the risk of elimination of unprotected (non-reserved) technical information security systems. In recent years, all surveyed banks have had a crash (failure) in any of the protection systems. In the majority of these failures were small and operationally removable in the course of the day. 43% of the banks, however, are faced with serious failures, which led to loss of information.

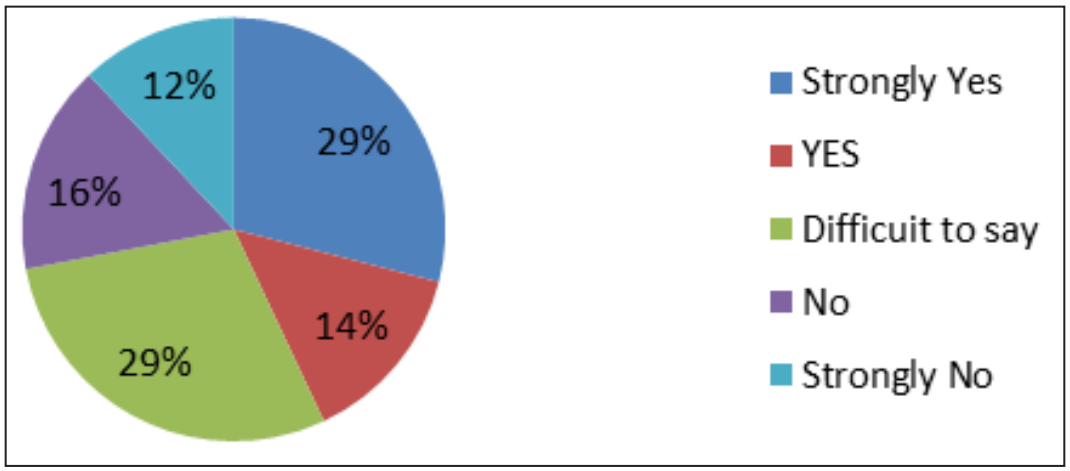

Fig. 1. Reliability of bank staff

The opinion of the bank security experts is unanimous that there are threats to the security of information inherent in both internal and external sources. Risky prove to be both intentional and unintentional actions of bank employees. Greater threat managers see in the unintended actions of the bank employees related to skipping certain security measures, indiscretion, imprudence, misunderstanding of certain processes, etc. Over the last three years in about 50% of the banks there has been a leak of information. Situations that provoke bank employees resort to outsourcing of information are too diverse. During the survey several potential hypotheses are distinguished related to the outsourcing of information that bank managers rated. In order to achieve a single assessment a numerical scale from one to five was introduced where five presents the highest degree of risk. So it came to getting the following answers:

Bank abuse by staff prone to export information have also been analyzed in relation to gender. Over 80% of the answers are that sex is not decisive. Most of employees in banks are women, but on the other hand men dominate in strategic positions with access to banking and sensitive information. Thus, the study showed that taking in mind the the proportion and distribution of women and man and alyzing cases of export of banking information - gender is not decisive, but rather the individual attitude of the individuals.

Situations were assessed where abuse of sensitive information can be carefully observed . The existence of such cases should signal a flare to the attention of information security officers.

Another potential for information leaks is the ability to use applications from the group of "Instant Messaging". Certain jobs positions would facilitate communication between bank employees and customers and counterparties of the bank. Only about 30% of the banks would manage such positions strictly limited and with no direct access to bank information. In none of these banks there have been detected a leak following this way. Security managers rated this kind of risk by 3.4 in the accepted scale for assessing risk and so estimated the potential risk of leaks using apps from the group "Instant Messaging".

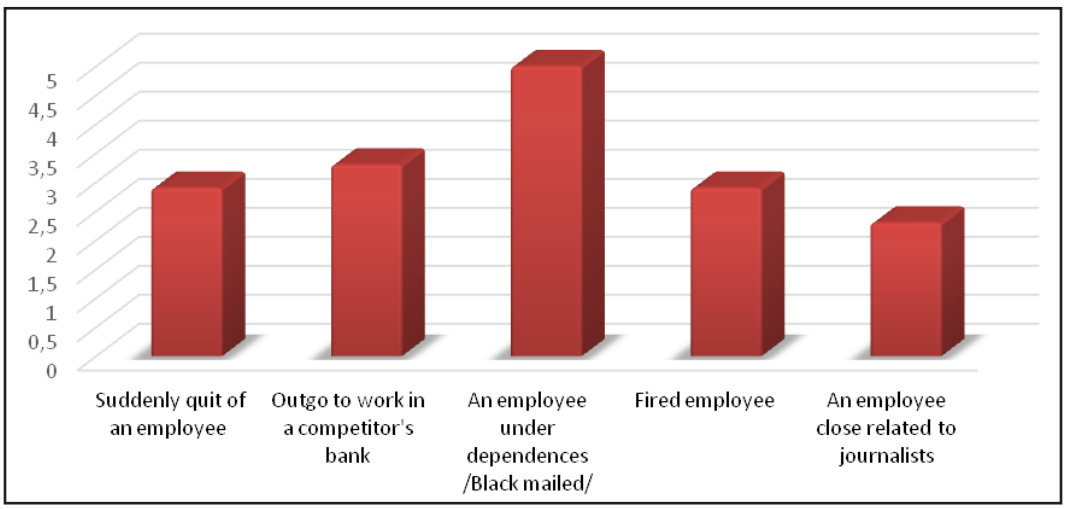

Fig. 2. Cases of information leaks

Next it was estimated the potential for leakage of information through the use of business and personal emails of employees. 14% of the banks established expiration of banking or sensitive information by sending unauthorized business emails. Bank employees in information security have not came through cases of loss of information due to incorrect attachment or wrong chosen recipient using email service. In about 30% of the banks at certain positions bank employees have got access to their personal e-mails. Attempts of abuse by that means have not been detected . The risk of leaks using e-mail is assessed by 3.9 points of maximum of 5 points (see. Figure 4).

Another alternative for those inclined to export data bank employees is to use various blogs and forums where intentionally or not they would comment on certain circumstances or would publish information identified as sensitive or even bank secrecy. Over the last three years about 30% of the banks have faced a similar problem.

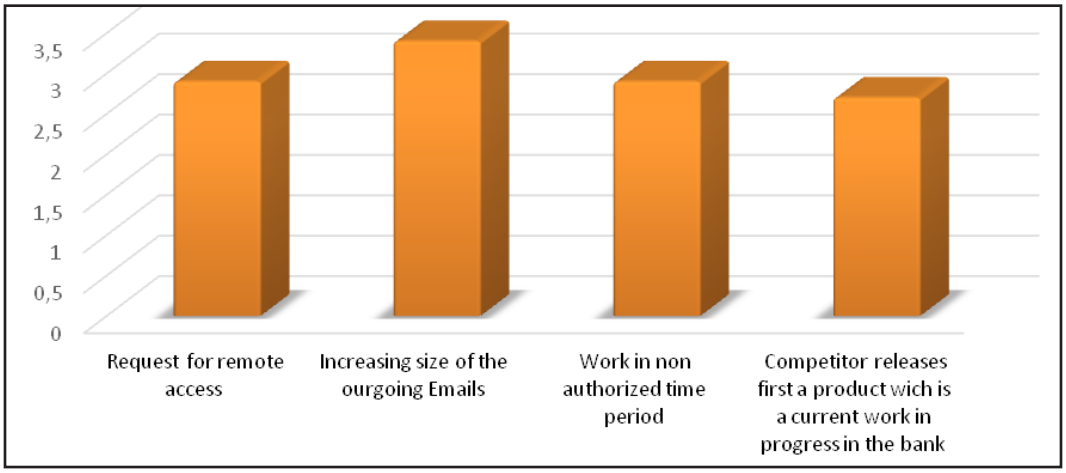

Fig. 3. Signalling for abuse

Serious threat to information security are external attacks relating to the interception of malware operational banking equipment. This kind of attacks strengthen their power and have created problematic situations in 43% of the banks. Of these, 29% of banks has sufferred loss of information and damaging its entirety. This risk of information loss is assessed as 3.1 points on the 5 grade scale by the surveyed Information Security managers.

Inevitably in carrying out daily activities in commercial banks FTP (file transfer protocol) is used for data transmission between the computers and the local banking network. In this direction again potential risk is found. Commercial banks, however, do not report leaks concerning FTP usage. It makes evident the efforts of the employees in the information security. Using LAN somewhat reduced attacks from malicious effects in this direction.

Another old and wide spread way of information export and transfer of information is on paper. For the past three years in the banking units of security this kind of offense has not been detected even though the assessment of its potential realization is high, namely - 4. Next, this kind of threat that is easy to implement is delivering information using a cell phone camera. 43% of the banks have experienced the realisation of this risk in the recent years.

The assessment of occurrence of this risk is estimated as 3.7 points.

Another problem for the banks is the loss of information due to improper storage of archival units. A few years ago the press news reported that the personal data of bank clients have exploded in the street near the containers in which the bank threw out their records. Only 14% of banks reported the realization of leaks due to improper storage and disposal of personal data and banking information.

Inevitably the carrying out the work activity of certain jobs requires the use of flash drives (accountanting operations, electronic signatures, etc.) And respectively that allows access to USB ports of a certain group of the computers at the bank. So they become an easy target for the occurrence of the risk of leaks by using removable media and other recording devices. Over 80% of banks reported that in the past three years they have not faced the realization of losses from this very kind, but question in open of whether it may occur. The assessment set by experts for the fulfillment of this risk is 3.6 points. The risk of data loss remains due to the quite possible physical loss or theft of devices such as memory sticks and laptops. In about 30% of banks in recent years key personnel lost information due to lost or stolen devices.

The risk of concealing information by accessing the proxy service and data encryption is assessed as possible with a score 3.1 points, but the currant banking practice in this country has not confronted such a problem for the time being.

Another serious risk with greater frequency of occurrence is draining credit and debit cards of bank customers. (c.Evers, 2012) Here the main problem lies in the actions of users of the cards. Much of the abuse debit cards is based on the fact that cardholders stored the plastic card and the PIN code at the same place. Thus, if bank customers would loose a wallet or it would be stolen, they greatly risk losing the money in the account if they don't block their accounts immediately. Understandably, diverse skimming devices are also been increasingly introduced into practice Another big threat is e-shopping online and using credit cards for payment. In about 50% of banks in the last three years the accounts of clients are becoming the object of attack. Customers undergone pre-phishing attacks related to gaining access to their electronic banking accounts and suffered abuse of their accounts are to be found in 86% of the surveyed banks.

Another object of a potential threat from malicious persons seeking access to information is the SQL server of the bank. Here the strong defensive efforts of the experts in information security are concentrated in answer to respectively serious attacks. About 30% of the banks have faced attacks leading to loss of information in recent years. As a result of this risk realisation all victims have sufferred an interruption of key business processes within their banks. Interruptions in large have been short but nevertheless damage was serious. At 14% of the surveyed banks the loss of data has been effected by offsetting the IP address of the computer bank.

Attempts to access bank information are made through telephone interviews with bank employees (about 30%). Thanks to the security measures introduced by banks namely clarifying questions about bank details, these attempts have not been successful.

We can make the following conclusion from figure 4: all these channels of info leaks have got relatively close results in estimation. The traditional export on paper remains the most risky of all. This fact suggests that the abusive person has access to a printer at any time to be able to print out sensitive information and to consequently delivered it

Fig. 4. Frequency of occurrence of various sources of risk of information leaks

without rising suspicion. Next ranks the risk of delivering information via email. We may conclude then that employees tend to abuse information using the easiest channels to carry out their deed without complicating it with blinding of data and transfer it to other information sources.

Following the risk assessment on the scale adopted, abuse performed through flash drives and mobile phones come the next in rank. Here again we find confirmation of the thesis that malicious employees choose the easiest and widely available channels. Access to personal phone is sacrosanct and hardly anyone would notice if the employee uses it for draining of information. Flash memory, whether personal or belonging to the company, is usually transmitted along with personal belongings of employees. So anytime information could be disseminated improperly.

The risk group mentioned above reaches nearly the assessment of the risk of attacks on the SQL engine of the banks where all banking data base is kept . Despite the serious defend undertaken by each bank the server is a subject of serious interest and more and more powerful attacks by hackers.

Next comes the risk of malware and interception of the IP of a PC at the bank. This kind of external threats find a way to pierce the strong protection of the information of the bank through more and more innovative methods and tools.

Along with powerful attacks from external sources, leakes through various instant messaging applications (where there is access to such) occupy the next place in the chart as well as the possibility of fraudulent use of FTP and retrieveing information from the bank server.

The risk group with the least value that commercial banks face is assessed to be the dissemination of sensitive information through blog posts and forums, telephone fraud and improper storage of archives. This assessment is at the lowest not because the level of threat is low but because better prevention can be carried out.(Data Breach Investigation Report, 2014, p.7)

4. Consequences

The outflow of banking information is accompanied by a number of tangible and intangible damage.

Firstly, leak means that there is outflowed and/or misconducted or even destroyed database. This is accompanied by costly recoveries of the database. These include:

- costs of setting up (updateing) software for data storage and of stregthening its protection;
- costs of payments for the developers of the software;
- costs of lost profits, covering the period of development and introducing of new software;
- time and costs for staff training.
- Secondly the work of the main business processes in the bank is hampered :
- lost profits realised due to difficulties in customer service of the bank;
- impaired quality of service to the bank customers;
- possible loss of abuse by clients in relation to establishing the amount of their assets.
- Thirdly, damage of the reputation of the bank.
- loss of customers› confidence in the bank and the subsequent outflow of customers and loss of financial assets;
- loss of a reliable source of income by large corporate clients;
- loss of future customers and serious financial damage;
- loss of key personnel due to poor reputation the bank;
- costs of hiring and training new staff.
- Fourth, distortions of the market positioning of the bank:
- Loss of financial stability;
- Bankruptcy of the bank.

5. Means for preventing the risk of leaks of information

Along with the introduction of appropriate software and high technical security measures banks in the country have to work on the basis of clear rules applicable to all bank employees, regardless of their work level. Rules for working with banking information and sensitive data must be based on:

- identification and classification of data and creation of appropriate measures for information security according to their type;
- regulatioins on the way of access to the data according to the position and the "need to know";
- proper data classification of date since the moment of their creation;
- prohibition of unauthorized use of (personal) devices in the network of the bank;
- information on portable devices such as laptops should be encrypted and possibility should be provided for it be to deleted remotely in case of theft;
- regular training of staff;
- checking staff awareness through various tests.

Conclusion

- The following conclusions can be drawn by the above research:
- The current state of commercial banks in Bulgaria shows a trend of stability and equilibrium;
- The level of bank security is high and constant investments are being made and measures taken to maintain the security of information;
- Given the results of the survey banks should not ignore the role of staff and its current conditions and hence they should work in the direction of preventing the outflow of bank information either willingly or not.
- Criminogenic factors group traditionally remained at a high level, thereby jeopardizing the integrity of bank assets as attacks on bank customers marked a significant size. This should motivate banks to strengthen the vigilance of its customers, giving them tips for ensuring high level of security.
- Condition of technical systems for information security must be under constant monitoring to face the growing threats from drilling firewall information security with more powerful and varied attack.
- Timely and appropriate safeguard measures would contribute to reducing the manifestation of the risk of leaks.

References

Antony,P., Melek, A., 2010, Data Leak prevention, ISACA.

Data Theft, 2009, Grand Thornton International LTD, Institute of Chartered Accountants in Ireland.

Data Breach Investigation Report, 2014, p.7

Dimitrov, S., 2011, Sigurnost na informatsiyata i do kakvo mozhe da dovede bezdeistvieto pri neinoto upravlenie, X-ta regionalna konferencia po Informatsionna sigurnost i sahranenie na danni, Sofia.

Evers, J., 2012, Details emerge on credit card breach.

Gordan, P., Data Leakge – Threats and Mitigation, SANS Institute, 2007, p5.

Keeney. M., 2005, Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors, United States Secret Service / CERT.

Social Dude, infirmacionna sigurnost, http://www.socialdude.net/bg