Journal of Business Studies Quarterly   jbsq.org

Comparative Analysis of Perceptions towards IT Security in Online Banking: Serbian Clients vs. Clients of Bosnia and Herzegovina

Nedim Makarević, Embassy of Bosnia and Herzegovina in Pakistan

Abstract

This study has been completed with a purpose to analyze and compare perceptions of clients of Bosnia and Herzegovina and those of Serbian clients about IT security in online banking, to provide insight into similarities and differences of their view points and to create important set of information for all subjects active in banking industry. Once the survey based on six variables and specific questions assigned to each one of those variables was prepared, results regarding both countries were collected and concluded. Survey was completed in both Bosnia and Herzegovina and Serbia at high response rates. Even 207 respondents replied from Bosnia and Herzegovina, while 227 respondents completed survey from Serbia. Results were analyzed and presented using descriptive statistics. Findings indicated that Serbian e-banking users do not trust to banks when it comes to IT security of online banking compared to clients of Bosnia and Herzegovina who provided higher trust level. It is important to mention that neither clients of Serbia nor clients of Bosnia and Herzegovina perceive tangible features as highly significant factors for their security. Results from both countries indicated that clients have lack of trust in online banking (especially in Serbia), and lack of awareness about personal tangible aspects that can improve security of personal online banking experience. The main limitation of this study is relatively small sample and too generic approach. Therefore, this study may be perceived as a pilot study for future researchers. The study's results may be of interest to marketers and managers of banks operating in Bosnia and Herzegovina and Serbia to learn more about their clients' perceptions towards their e-banking services. Considering gap in literature when it comes to research dealing with IT-security of online banking in both Serbia and Bosnia and Herzegovina, this article is not only unique, but it may be stimuli for new research with different approaches in the future.

Keywords: *Perceptions, IT security, online banking*
JEL Classification: D82, G2

1. Introduction

Handling money from comfortable house atmosphere is standard and normal everyday activity for many people all around the world. This way of maintaining money with no physical contact and making money transactions is known as "online banking". There are many definitions of online banking provided by many researchers, but all of them have some main

elements which are within the following definition, provided by Muniruddeen Lallmahamood (2007). He defined internet banking as banking services over the public network (the Internet), through which customers can use different kinds of banking services ranging from the payment of bills to making investments. Internet banking or online banking has created new ways of handling banking transactions for banking related services and for e-commerce related transactions such as online shopping (Lallmahamood, 2007).

However, development of handling money with no physical contact did not provide new opportunities only to clients, but to criminals as well. In fact, criminals are able to steal money with no physical contact and any tangible evidence remaining after their criminal transaction. In other words, they can conduct the robbery in their pijamas from their bed rooms. Knowing this fact turn on red alarm in heads of many clients. As banks' dependence on new technologies increases, their need to protect their own and assets of their clients increases as well. This is where importance of IT security for banks' clients starts. For this reason, it is of crucial importance for banks as provider of online banking services, to know awareness level and perceptions of their clients towards IT security of online banking. Since results of this research will enable banks to learn more about their clients, this research have potential to be important source of information for consideration by banks when it comes to their planning and development activities. If we consider gap in the literature on this issue in both countries, Bosnia and Herzegovina and Serbia, this article becomes even more valuable.

Results regarding both countries are collected and concluded after preparing survey based on six variables and specific questions assigned to each one of those variables. The survey was distributed to clients who are actively using online banking. It was completed in both Bosnia and Herzegovina and Serbia at very high response rates. Even 207 respondents replied from Bosnia and Herzegovina, while 227 respondents completed survey from Serbia. Results were analyzed and presented using descriptive statistics. The main objective of this paper was to analyze and compare perceptions of Bosnian and Serbian clients about IT security in online banking, to provide insight into similarities and differences of their view points and to create important set of information for all subjects active in banking industry.

In the following sections of this work, through theoretical background, all necessary definitions along with brief historical facts important for understanding this topic will be explained. Accordingly, information on online banking in Bosnia and Herzegovina and Serbia as countries in focus will be provided so readers can be more familiar with the situation in these states. Reason for selecting these two countries is their unique history. Both of the states were in a war in near history, and both of them are striving to become a member state of European Union. After explaining used methodology, results will be analyzed, discussed and concluded.

2. Theoretical background

Muniruddeen Lallmahamood (2007) defines internet banking as banking services over the public network (the Internet), through which customers can use different kinds of banking services ranging from the payment of bills to making investments (Lallmahamood, 2007). On the other hand, Jagdeep Singh (2012) defines internet banking as online systems which allow customers to plug into a host of banking services from a personal computer by connecting with the bank's computer over the telephone wires. He is also mentioning some synonyms for internet banking such as online banking, PC banking, home banking or electronic banking (Singh, 2012).

According to Gordon and Loeb (2002), Information security is concerned with the protection of three characteristics of information: confidentiality, integrity, and availability through the use of technical solutions and managerial actions (Gordon & Loeb, 2002).

Banks are not only dealing with intangible money transactions, but also with protection of highly sensitive information such are credit cards' PINs, data about the customers, customers bank accounts and all other kinds of information that could enable to third party conducting the criminal activities and making damage for both, customer and bank. According to Landwehr (2001), weaknesses of banks' information systems are named vulnerabilities, and it is likely that such vulnerabilities represent opportunities for crime by third parties (Landwehr, 2001).

One of the alternatives when it comes to keeping money in safer forms than cash is electronic handling of money, where no physical contact is necessary. This means that almost all transactions can be realized via different devices including computers, mail or telephone, without physical contact. Such an operation resulted in new types of crime, and some of them are still new to the legal systems. Main problem is that allowing people to make transactions with no physical contact opens the door for criminals to gain access and make transactions. Accordingly, beside the physical security systems of banks, possibility of crime is still very high. Sometimes, in order to keep public image, banks do not even investigate and prosecute cybercrimes. If they would do that, customers wouldn't deposit money in their banks (Pfleeger & Pfleeger, 2006). In short, big question emerge in heads of clients: "Is electronic way of handling money safe?"

3. Briefly about online banking in Serbia & Bosnia and Herzegovina

In the following two sections, online banking will be explained more specifically regarding every country individually.

3.1 Online banking in Serbia

According to Mirjana Knežević and Aleksandar Lukić (2012), banking system in Serbia in the past period depends on its development of sociopolitical situation and economic changes in the country. The period of transition of banking sector in Serbia begun in 1992, but the most significant changes have been occurring after 2000 when country was quite ready for foreign direct investment. Development of e-banking in Serbia can be followed from perspective of usage. According to data of National Bank of Serbia, up to 2003, there were issued less than 400 thousand debit cards in Serbia, and already in 2005, the number of cards in circulation reached 3,8 million. The development of electronic banking in Serbia has been continued so that it is relatively well developed today, with tendencies of further intensive development by types of products and technological level of possibility of its usage (Lukić et al, 2012).

Tijana Radojevic and Dalibor Radovanovic (2010) stated taht in economically developed countries, percentage of e-banking in payment system is very high (e.g. in France, 70 and 80 %), while Serbia is much lower (about 1/3). They added that current IT infrastructure is underdeveloped in Serbia. Additionally, although it is not recorded any case of fraud in terms of online banking, many people in Serbia are still very skeptical when it comes to security. Authors concluded that it is necessary, however, to educate customers, in order not to happen that easily fall into traps hacker in the future which will inevitably be (Radojević and Radovanović, 2010). Serbia also developed new legal framework that was builded as follows: 1) The Law on Electronic Signature enacted in 2004; 2) The Law on Electronic Commerce enacted in 2009; 3) Law on Payment Transactions (Radovanović & Milošević, 2010).

Group of authors Sarac, Radojevic, Stanisic, Adamovic, Radovanovic (2012) wrote on safety of e-business Applications in Serbia: Applied Knowledge Based on SSL Traffic. They presented and analyzed current problems of e-business in the implementation of SSL computer network protocol. Their paper presents research results on attacks on e-business and computer systems. These authors were dealing with three hypothesis. First one says that lack of assurance about security is the greatest barrier currently affecting the growth of e-business applications. In fact, e-business application users must have confidence that their electronic transactions will remain private and unaltered, and they must trust the system to prevent fraud. Second hypothesis states that e-business application security measures involve interaction of users, hardware, and software. This is important because all security issues which are inseparable of e-business applications have to be adressed. Hypothesis three says that model used in this research on safety of e-business applications will be able to identify security breach and alert the users on potential fraud. After analyzing contemporary methods of protection and pointing out their shortcomings, authors presented actuality of the mentioned problem and contributed to aforementioned security deficiency resolving (Sarac, Radojevic, Stanisic, Adamovic, Radovanovic, 2012).

Predrag Radovanović & Andriana Milošević (2010) summarized current situation as well as the possibilities for future development of electronic banking in Serbia, and reviewed available services in domain of internet and mobile banking. Authors emphasized that organization of new national payment infrastructure has been one of the key reforms in Serbia following the restitution of its membership in the United Nations, the International Monetary Fund, the World Bank and other international organizations. Radovanović and Milošević also explained that former payment operations system in Serbia has been built around the Clearing and Payments department which was state owned institution that maintained the accounts of all economic operators in country. This institution was in charge of all payment and clearing operations. Big move for Serbia was in year 2001 when all responsibilities for payment operations from Clearing and Payments Department has been given to commercial banks. Beside this, their paper also presents detailed statistical data on payment cards operations in Serbia, as well as data on transactions volume in RTGS and clearing systems (Radovanović & Milošević, 2010).

When Tijana Radojevic & Dalibor Radovanovic (2010) spoke about this issue, they concluded that current law regulations of Serbia and related solutions are disabling faster development of electronic services and represent stagnation for it's further development, because some areas (which would provide faster and more dynamic electronic services development) of e-business domain are not regulated. Regardless of this, authors stated that in Serbia almost all commercial banks offer some sort of electronic banking to their customers. Still, current information technology infrastructure is underdeveloped according to Radojević and Radovanović. On the other hand, competition force banks to improve their situation and offer more convenience for their customers. Accordingly, banks provide their services in a variety of ways in Serbia. For instance, via home computer, mobile phone users are able to access account balance, view transactions, view statements of changes etc. (Radojevic & Radovanovic, 2010).

Mirjana Knežević, Aleksandar Lukić (2012) considered this issue in broader target and they focused not only on Serbia, but also on its neighboring countries. The subject of their work is the analysis of electronic banking in Serbia and the neighboring countries, their legal regulations and applications in the banking system. These authors started with the fact that contemporary banking business range over great number of new banking products and services

from thee area of electronics banking. They related development of electronic banking in Serbia with the socio political situation & economic changes in Serbia which started in 1992. However, after year 2000, along with arrival of foreing investors, huge changes in property relations occur. This transformation changed the way of organizing, managing all aspects of banking businesses. Lukić and Knežević thinks that these development phases in banking industry played curcially important tole for accelerated development of the electronic banking and satisfying needs of clients (Lukić & Knežević, 2012).

3.2 Online banking in Bosnia and Herzegovina

The biggest expansion in terms of online banking development happened in Bosnia and Herzegovina in year 2010 when there was 19.257 business subjects and 48.545 citizens using the online banking (Central Bank of BiH, 2010)

According to report of Central Bank of Bosnia and Herzegovina in 2013, internet banking has increased for 23.11 percentage compared to previous years. Still, this information is not perceived as significant increase by Central Bank of Bosnia and Herzegovina (Central Bank of BiH, 2013).

One year later, new report of Central Bank of Bosnia and Herzegovina prepared in year 2014 did not bring some extraordinary different results. Still, even though there is an increase in both, number of banks offering electronic banking and number of users, the increase trend is not impressive. In 2014, the number of electronic banking users was 213.562, while even 25 banks were offering this type of service. This number of users is only 0.01 % of total number of cards in the country, which is the main reason why the Central Bank is not impressed with this fact (Central Bank of BiH, 2014).

4. Literature review

According to Shrinath (1997), „information is power "has nowhere been realized more significantly than in the banking industry. When discussing the risks and challenges for IT security in that period of time, Shrinath mentioned four risks: unauthorized system/data access by business users in the bank; unauthorized system/data access by application/system support personnel; unauthorized system/data access by customers; unauthorized system/data access by the public at large. Since most people do not realize that large banks are prone to high risk of security breakdown even without going so far as the Internet, author decided to examine and explain the most critical areas (Shrinath, 1997).

Lawrence A. Gordon and Martin P. Loeb (2002) wrote an article which presents an economic model that determines the optimal amount to invest to protect a given set of information. Their model takes into account the vulnerability of the information to a security breach and the potential loss should such a breach occur. After analysis conducted by Gordon and Loeb (2002), they suggested that in order to maximize the expected benefit from investment in information protection, a firm should spend only a small fraction of the expected loss due to a security breach (Gordon & Loeb, 2002).

Authors found very important to know about perceptions of users about specific technologies. This is how technology acceptance model was born. Pikkarainen et al. (2004) conducted a study about consumer acceptance of online banking. They investigated online banking acceptance in the light of the traditional technology acceptance model (TAM). The data for their results was consisted of group interview with banking professionals, TAM literature and e-banking studies. According to their results, perceived usefulness and information on online banking on the Web site were the main factors influencing online-banking acceptance (Pikkarainen et al., 2004).

When it comes to explanation of basic concepts involved with system security, helpful was introductory chapter of book entitled „Security in computing "written by Charles P. Pfleeger & Shari Lawrence Pfleeger (2006). Their book deals with broad range of computer security related topics such are: cryptography; secure systems development; basic communications technologies; advices on planning, risk, and policies; Intellectual property; computer crime, and ethics. In short, it is possible to conclude that this book can serve as great guide to information about computer security attacks and countermeasures (Pfleeger & Pfleeger, 2006).

Interesting research was made by Luis V. Casalo, Carlos Flavian and Miguel Guinaliu (2007) who conducted it with purpose to analyze the influence of perceived web site security and privacy, usability and reputation on consumer trust in the context of online banking. Their paper described the positive effects of security and privacy, usability and reputation on consumer trust in a web site in the online banking context. This study is very interesting and valuable since it proposes link between security, privacy and trust, amongst others, in the online banking context (Casaló et al., 2007).

Muniruddeen Lallmahamood (2007) explored the impact of perceived security and privacy on the intention to use Internet banking. He used an extended version of the technology acceptance model (TAM) is to examine the above perception and concluded that while perceived usefulness is a critical factor in explaining users' intention to use Internet banking, it is important to pay attention to the security and privacy of users' of Internet banking. According to results, convenience, ease and time saving are the main reasons for the adoption of Internet banking, whereas security, trust and privacy appear to be the top main concerns for non-Internet banking users. As author mentioned, this may also imply that security concerns and privacy protection are perceived to be part of the overall service provided by the Internet banking services providers, and he suggests that banks should gain customers' confidence through raising security levels of the bank (Lallmahamood, 2007).

Many studies that are dealing with evaluation of clients' trust when it comes to banking are including „security" as important construct. This leads to conclusion that IT security is important for getting customer's trust in banking business. Yap, K. B., Wong, D. H., Loh, C., & Bak, R. (2010) wrote a paper with aim to examine the role of situation normality cues (online attributes of the e-banking web site) and structural assurance cues (size and reputation of the bank, and quality of traditional service at the branch) in a consumer's evaluation of the trustworthiness of e-banking and subsequent adoption behavior. One of their findings in this work stated that web site features that give customers confidence are significant for promotion of e-banking (Yap et al., 2010).

Research found to be very useful for this article is the one completed by Mohanad Halaweh (2012) who was writing about user perceptions of e-commerce security (Halaweh, 2012). In fact, both online banking and e-commerce are having common characteristic which is no physical (face to face) contact between parties involved in transaction, and using same technologies for doing transaction. This means that both of them are exposed to same risks. Accordingly, this common characteristic was very useful while identifying relevant variables for this study since some of them are simply modified and used for this research. Results of study conducted by Mohanad Halaweh (2012) showed that user characteristics, psychological state and intangible security features have a significant influence on e-commerce security perception. Additionally, in contrast, tangible security features and cooperative responsibility have a non-significant influence (Halaweh, 2012).

Singh (2012) commented that customers, both corporate as well as retail ones are no longer willing to queue in banks, or wait on the phone, for the most basic of services. Therefore, electronic delivery of banking services is becoming the ideal way for banks to meet their clients' expectations. Accordingly, author got idea to study the scenario of e-banking, and in his study he considered opinions of 100 customers from Ludhiana. The results of this work revealed that people are aware of e-banking, but not fully. In fact, the Customers are at ease after using e-banking since it saves the precious time of the customer. It has also been found that Customer satisfaction varies according to age, gender, occupation etc. (Singh, 2012).

5. Variables & survey

For conducting this research, with aim to get closer insight into clients' perceptions towards online banking in Serbia and BiH, six variables were identified as a result of literature review. Those variables are as follows:

5.1 Privacy aspect refers to confidence in the technology and online banking service provider when it comes to protection against privacy issues such are private information of client, information about money transactions conducted by client, information about client's personal passwords etc. Pikkarainen et al (2004) stated that as the amount of products and services offered via the Internet grows rapidly, consumers are more and more concerned about security and privacy issues (Pikkarainen et al., 2004).

5.2 Control aspect - When it comes to control perspective of IT security, as it is possible to conclude from survey questions of Yap, K. B., Wong, D. H., Loh, C., & Bak, R. (2010), this aspect refers to strictness of identity ascertaining when sending messages to client, or doing transactions by client, but also general control by bank when it comes to online transactions' confidentiality (Yap et al., 2010).

5.3 Psychological aspect - According to Halaweh, Mohanad (2012) The psychological aspect of security incorporates the feeling of fear, the need to feel that one's money is secure, and the ability to control the payment process and performance of online transactions. Even though he made research about e-commerce, because of same nature of e-commerce and e-banking which is remote rather than face-to-face, his work was useful for preparation of survey in this study (Halaweh, 2012).

5.4 Therefore, it is possible to conclude that many customers have the misconception that the use of e-banking is vulnerable and that there is a high probability that their money will be lost.

5.5 Tangible features - Halaweh, Mohanad (2012) defines tangible indicators as those technological security features of websites that can be checked by users, such as https, padlocks and security certificates. Tangible features need to be understood and checked by the customer over the website rather than captured through social communication; this involves having knowledge and experience of these features, such as knowing what a security certificate means and how to check whether it has expired (Halaweh, 2012).

5.6 Intangible indicators - When talking about intangible indicators such are famous website and reputation, Halaweh, Mohanad (2012) says that they are not seen on the website and cannot be directly checked over the website. They are affected by society in terms of communication and the environment: where the customer lives and what they hear from others, as well as their past experience (Halaweh, 2012).

5.7 Perceived IT security Perceived IT security refers to general perception of online e-banking services by clients when it comes to IT security.

Accordingly, survey consisted of twenty questions was created. Questions were mainly adapted from previous researches considering Pikkarainen et al (2004), Casaló, Flavián, and Guinalíu (2007), Yap, K. B., Wong, D. H., Loh, C., & Bak, R. (2010), Halaweh, Mohanad (2012), Muniruddeen Lallmahamood (2007). All questions prepared for the survey, along with their references they were adapted from, are presented in Table 1 available in the next page.

Pikkarainen et al. (2004) conducted group interview with banking professionals in order to learn about consumer acceptance of online banking (Pikkarainen et al., 2004). Specific questions related to privacy aspect from his interview were adapted and used in this research to examine clients' concerns about their privacy and security issues in e-banking. Casaló, Flavián, and Guinalíu (2007) made research with purpose to analyze the influence of perceived web site security and privacy, usability and reputation on consumer trust in the context of online banking (Casaló et al., 2007). Since they are dealing with similar issue, questions regarding security and privacy were adapted and used in this study. Yap, K. B., Wong, D. H., Loh, C., & Bak, R. (2010) used survey to evaluate trustworthiness of e-banking and subsequent adoption behavior through several factors (Yap et al., 2010). Accordingly, several questions helpful to measure control aspect of IT security in e-banking were used in our study. Halaweh, Mohanad (2012) studied user perceptions of e-commerce security (Halaweh, 2012). Since both e-commerce and e-banking are having the same characteristics such is lack of face to face communication and physical contact which implies same issues and concerns for final users of such a services, many questions were adapted from his survey in order to measure psychological aspect, tangible and intangible indicators, and perceived IT security in general when it comes to online banking. Also, when it comes to Muniruddeen Lallmahamood (2007), one of questions used in his study was useful to adapt for this research when it comes to measuring psychological aspect of IT security (Lallmahamood, 2007).

Questions	Adapted from
I trust in the ability of bank to protect my privacy	Pikkarainen et al (2004)
I am not worried about my personal information given to bank	
I think that my bank's information system respects personal data protection laws	Casaló, Flavián, and Guinalíu (2007)
I think that my bank's information system will not provide my personal information to other companies without my consent	
I think that my bank's information system respects user's rights when obtaining personal information	
I think that bank needs to ascertains my identity before sending any messages to me	Yap, K. B., Wong, D. H., Loh, C., & Bak, R. (2010)
I think that bank needs to ascertains my identity before processing any transactions received from me	
I trust that my bank uses security controls for the confidentiality of online transactions	
I don't fear when I am using e-banking services	Halaweh, Mohanad (2012)
I never have misconceptions about using e-banking services	
I don't feel anxious to use e-banking services because of its nature, which involves a lack of face-to-face communication	
I feel safe when I release credit card information through Internet banking	Lallmahamood, Muniruddeen (2007)
I don't check the presences of http(s) in the URL when I handle money transactions online	Halaweh, Mohanad (2012)
I don't check the small padlock icon on the bottom right corner of the website when I handle transactions online	
I don't check the digital security certificate of the web site when I handle money transactions online	
I would use e-banking services only provided by on a reputable bank	Halaweh, Mohanad (2012)
I would use e-banking services only provided by local bank	
I think my bank shows great concern for the security of any online transactions	Casaló, Flavián, and Guinalíu (2007)
I believe using e-banking services online is secure	Halaweh, Mohanad (2012)
Using e-banking services gives me a feeling of security	

Table 1. Review of survey questions

6. Data and Methodology

Data for this study was collected by the means of a survey conducted in Serbia and Bosnia and Herzegovina in 2013. A total of 500 questionnaire forms were delivered to respondents in both countries. Half of the surveys (250) was delivered to Bosnia and Herzegovina, while half (250) was delivered to Serbia. Most of surveys were answered with good response rates. In Serbia even 227 respondents out of 250 completed the survey giving a response rate of 90.8 percent. Situation was slightly worse in Bosnia and Herzegovina since 207 clients out of 250 completed the survey giving a response rate of 82.8 percent.

Surveys were filled at universities by students, academic and administrative staff, and in branches of different institutions of Serbia and Bosnia and Herzegovina by randomly selected clients. This resulted in a sample that was well distributed in terms of demographic information (e.g. age, and education).

Data is mainly numerical except demographics part which is categorical. Seven point Likert scale was used in order to test the agreements of the respondents on six variables through twenty questions. The collected data is then inserted into an excel spreadsheet and analyzed descriptively. The surveys were distributed both online and personally. Online version of survey was created, and its link was sent via e-mail to potential participants.

7. Results
7.1 Demographics

Demographics information includes respondents' department, positions within the department and their education levels, gender and age. When it comes to gender, in both Serbia and Bosnia and Herzegovina, there was more male respondents. Detailed information on gender are presented in figure 1 presented below.
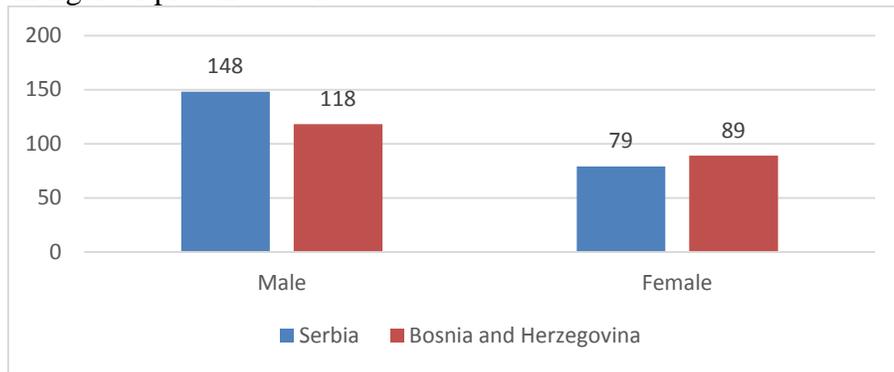
Figure 1. Gender of respondents

When it comes to educational background of respondents, in both countries more than 50% of surveyed respondents had undergraduate degree. Around 60 respondents of both countries (Bosnia and Herzegovina - 53; Serbia - 67) had Master degree and only few had a PhD level (Bosnia and Herzegovina – 4; Serbia – 10). Twenty one out of all surveyed respondents in Bosnia and Herzegovina did not have higher education, while 33 of surveyed respondents in Serbia had the same status.
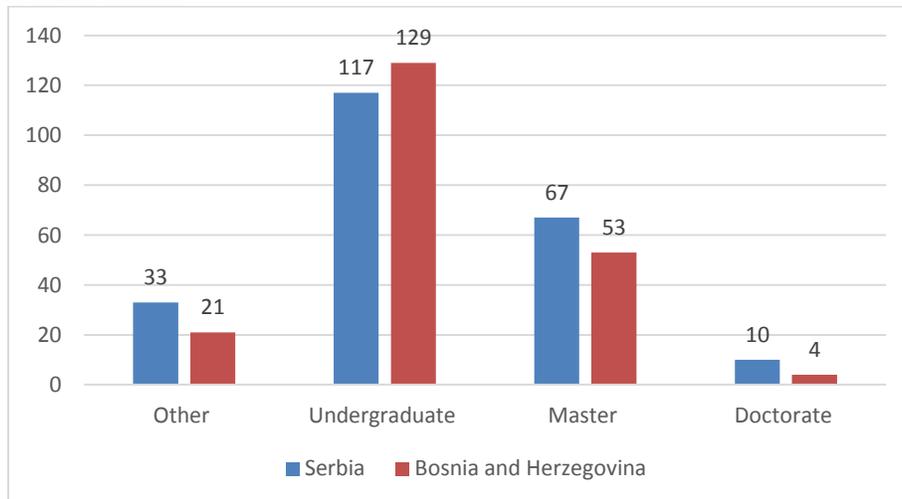
Figure 2. Educational background of respondents

When it comes to job positions of respondents, since surveys have been distributed to clients who are working in various institutions of Bosnia and Herzegovina and Serbia, sample is

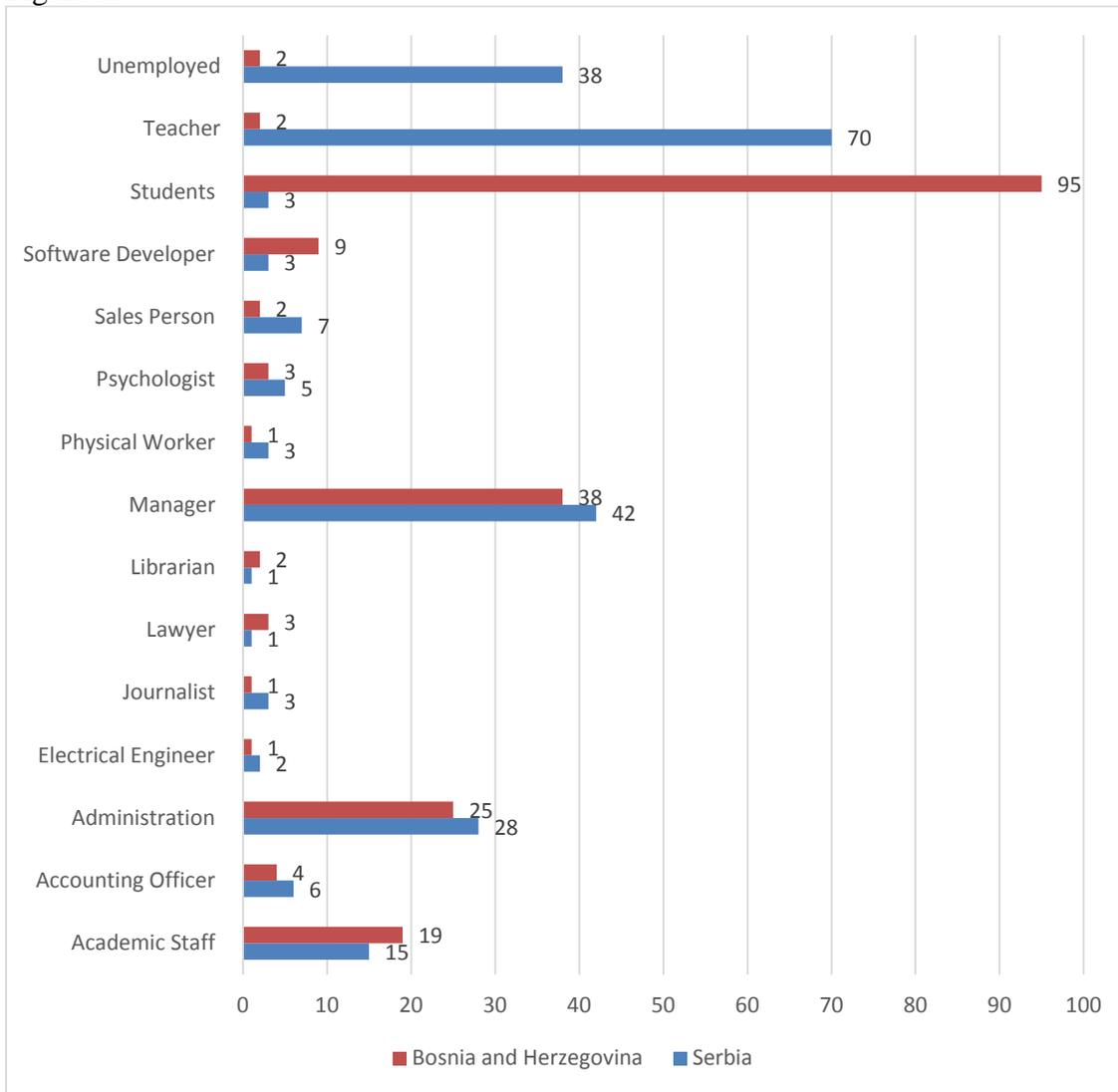well distributed in this aspect. All details regarding job positions of respondents are presented in Figure 3.

Figure 3. Job positions of respondents

7.2 Survey results

Before interpretation of results, to assure that reader will properly understand all tables and related explanations, it is important to explain interpretation values for used 7 point Likert scale. The meaning of interpretation values is as follows:

- 1 – Respondent strongly disagrees with the statement

- 2 – Respondent disagrees with the statement
- 3 - Respondent slightly disagrees with the statement
- 4 – Respondent is neutral (he/she neither agrees not disagrees with the statement)
- 5 – Respondent slightly agrees with the statement
- 6 – Respondent agrees with the statement
- 7 - Respondent strongly agrees with the statement

From Table 2, it is possible to conclude that privacy aspect of IT security in online banking is perceived as less acceptable by clients of Serbia compared to those of Bosnia and Herzegovina (BiH). In fact, mark of 5.223 indicates that clients of Bosnia and Herzegovina slightly agreed that banks are able, and doing their best to protect their privacy. Results from Serbia indicated that privacy aspect of IT security in online banking of Serbia is perceived as not trustable, worrying and with no respect to personal information of clients.

Variable: Privacy aspect	Mean	
Questions	BiH (5.223)	Serbia (3.480)
I trust in the ability of bank to protect my privacy	5.338	3.466
I am not worried about my personal information given to bank	5.188	3.885
I think that my bank's information system respects personal data protection laws	5.370	3.486
I think that my bank's information system will not provide my personal information to other companies without my consent	5.059	3.334
I think that my bank's information system respects user's rights when obtaining personal information	5.159	3.23

Table 2. Privacy aspect

When it comes to control aspect, by agreement with offered statements, Bosnian clients think that high level of control is necessary. Their answers regarding statements in this variables was close to 6 in all cases, which means that clients from BiH agreed with statements about ascertaining their identities while using online banking and they believed that banks are using security controls to improve confidentiality of online transactions (Table 3). Serbian clients slightly agreed with statements about ascertaining their identities while using online banking and they slightly believed that banks are using security controls to improve confidentiality of online transactions.

Variable: Control aspect	Mean	
Questions	BiH (5.594)	Serbia (4.968)
I think that bank needs to ascertains my identity before sending any messages to me	5.585	5.475

I think that bank needs to ascertains my identity before processing any transactions received from me	5.667	4.897
I trust that my bank uses security controls for the confidentiality of online transactions	5.532	4.532

Table 3. Control aspect

When it comes to psychological aspect whose results are presented in Table 6, Bosnian clients' perceptions towards offered statements is within "slight agreement" region. This indicated that they are to some extent paranoiacs, and that there is fear, misconceptions and anxiety exist while using online banking. On the other hand, situation in Serbia appeared to be very interesting. Serbian respondents disagreed or slightly disagreed with the statements which leads to conclusion that fear, misconceptions and anxiety while using online banking, but also feeling of unsafety when releasing credit card information through internet banking exist.

Variable: Psychological aspect	Mean	
Questions	BiH (5.221)	Serbia (2.452)
I don't fear when I am using e-banking services	5.322	2.343
I never have misconceptions about using e-banking services	5.345	3.037
I don't feel anxious to use e-banking services because of its nature, which involves a lack of face-to-face communication	5.285	2.475
I feel safe when I release credit card information through Internet banking	4.932	1.952

Table 4. Psychological aspect

Results showed that Bosnian clients are not completely aware of importance of tangible features for security while doing online transactions. In fact, clients were mainly slightly agreeable with the statements which indicated that they are not very careful when it comes to paying attention to presence of http(s) in the URL and small padlock icon. When it comes to digital security certificate of the web site, they were neutral which gives information that they pay attention to this specific aspect of online banking IT Security. Results from Serbian clients showed that they are also not completely aware of importance of tangible features for security while doing online transactions. Respondents slightly agreed with statements that they are not very careful when it comes to paying attention to presence of http(s) in the URL, small padlock icon and digital security certificate of the web site. When it comes to digital security certificate, they were neutral. More details about this aspect are available in Table 5.

Variable: Tangible features	Mean	
Questions	BiH	Serbia

	(4.563)	(4.637)
I don't check the presences of http(s) in the URL when I handle money transactions online	4.715	4.669
I don't check the small padlock icon on the bottom right corner of the website when I handle money transactions online	4.536	4.879
I don't check the digital security certificate of the web site when I handle money transactions online	4.439	4.362

Table 5. Tangible Features

This research showed that marketing and intangible assets of banks are slightly influential in Serbia. Clients are paying more attention to tangible rather than intangible ones such are banks' reputation, location and its concern towards security provision for its clients when making their decision to use online banking services. According to results, this is not the case in BiH. Marketing and intangible assets of banks are quite influential in this country. Bosnian clients are paying more attention to intangible features such are banks' location and its concern towards security provision for its clients when making their decision to use online banking services. This is not the case with the bank's reputation in eyes of Bosnian clients. More details about influence of intangible features to clients' perceptions of IT security of online banking are available in Table 6.

Variable: Intangible features	Mean	
Questions	BiH (5.051)	Serbia (5.312)
I would use e-banking services only provided by on a reputable bank	4.955	6.546
I would use e-banking services only provided by local bank	5.048	5.342
I think my bank shows great concern for the security of any online transactions	5.150	4.049

Table 6. Intangible features

When it comes to general opinion about IT security of online banking, from Table 7, it is possible to conclude that Serbian clients slightly disagreed with the statements which leads to conclusion that they do not believe that usage of e-banking services online is secure, and they do not use e-banking services with feeling of security. Bosnian clients didn't have specific opinion about the mentioned statements, and showed that they do not completely believe in secure online banking.

Variable: Perceived IT security	Mean	
Questions	BiH (5.208)	Serbia (4.148)
I believe using e-banking services online is secure	5.188	4.327
Using e-banking services gives me a feeling of security	5.227	3.696

Table 7. Perceived IT security

8. Conclusion

This research provided important insights about clients' perceptions towards IT security of online banking in Serbia and Bosnia and Herzegovina (BiH). Careful comparative analysis of results collected from these two countries has been conducted. Response rate was good in target samples, 90.08% in Serbia and 82,8% in BiH. Fact that surveyed people are coming from various companies, departments and positions within those departments gives even more importance and value to the results of this work. Limitations of this research are relatively small sample and quite generic approach to problem. Accordingly, recommendations for future researches would be based on going more deeply into the issue and analyzing larger samples. This article represents very unique set of information for the banks already operating in Serbia and BiH, or having tendency to start business in these countries. This research empirically proved that clients of Serbia and BiH do not have same perceptions towards online banking, but still they have similar opinions in some aspects. Serbian clients are with intensive fear and misconceptions, not aware of tangible features' importance, thinking that banks are not able to protect their privacy completely and that banks are not doing their best to improve confidentiality of online transactions. Clients of BiH also do not think that banks are able to protect their privacy completely. They agree and trust to bank when it comes to control aspect, but still there is certain amount of feeling unsafe in psychology of people which could be the reason why there is no significant increase in trend line of electronic banking development of BiH. The fact that both Serbian and Bosnian clients are not very informed about importance of tangible features of IT Security in online banking leads to implication for banks to work more in order to improve awareness of people and stress importance of this issue in conducting online transactions. Intangible features were of medium importance for Bosnian clients, and in general they slightly believe and feel that online banking is secure. Are these differences related to different development levels in economies of BiH and Serbia, these could be good questions for some other future research.

References

Casalo, L., Flavian, C., & Guinaliu, M. (2007). The role of security, privacy, usability and reputation in the development of online banking. *Online Information Review, 31*(5), 583-603.

Central Bank of BiH. (2010). *Annual Report.* Sarajevo: Central Bank of BiH. Retrieved from http://cbbh.ba/index.php?id=36&lang=bs

Central Bank of BiH. (2013). *Annual Report.* Sarajevo: Central Bank of BiH. Retrieved from http://cbbh.ba/index.php?id=36&lang=bs

Central Bank of BiH. (2014). *Annual Report.* Sarajevo: Central Bank of BiH. Retrieved from http://cbbh.ba/index.php?id=36&lang=bs

Gordon, L., & Loeb, M. (2002). The Economics of Information Security Investment. *Transactions on Information and System Security, 5*(4), 438–457.

Halaweh, M. (2012). Modeling user perceptions of e-commerce security using partial least square. *Journal of Information Technology Management, 23*(1).

Lallmahamood, M. (2007). An Examination of Individual's Perceived Security and Privacy of the Internet in Malaysia and the Influence of This on Their Intention to Use E-Commerce: Using An Extension of the Technology Acceptance Model. *Journal of Internet Banking and Commerce, 12*(3).

Landwehr, C. (2001). Computer security. *International Journal of Information Security, 1*(1).

Lukić, A., & Knežević, M. (2012). Electronic Business Operations on the Banking Market in Serbia and Countries in the Region. *International Journal of Advances in Management and Economics, 1*(4).

Pfleeger, C., & Pfleeger, S. (2006). *Security in Computing* (4 ed.). Prentice Hall.

Pikkarainen, T., Pikkarainen, K., Karjaluoto, H., & Pahnila, S. (2004). Consumer acceptance of online banking: an extension of the technology acceptance model. *Internet Research, 14*(3), 224–235.

Radojevic, T., & Radovanovic, D. (n.d.). E-Banking implementation in Serbia. *6th International Scientific Conference.*

Radovanović, P., & Milošević, A. (2010). Current state and prospective development of electronic banking in Serbia. *Economics and Organization, 7*(1).

Sarac, M., Radojevic, T., Stanisic, N., Adamovic, S., & Radovanovic, D. (2012). Safety of e-business Applications in Serbia: Applied Knowledge Based on SSL Traffic. *Journal of Internet Banking and Commerce, 17*(3).

Shrinath, B. (1997). Information Security in Banks. *Journal of Financial Crime, 5*(1), 65-71.

Singh, J. (2012). Scenatio of e-banking in today's life - A Survey. *International Journal of Computing & Business Research.*

Yap, K., Wong, D., Loh, C., & Bak, R. (2010). Offline and online banking – where to draw the line when building trust in e-banking? *International Journal of Bank Marketing, 28*(1), 27-46.