ENTREPRENEURSHIP AND SUSTAINABILITY ISSUES
ISSN 2345-0282 (online) http://jssidoi.org/jesi/
2019 Volume 6 Number 4 (June)
http://doi.org/10.9770/jesi.2019.6.4(31)

Publisher
http://jssidoi.org/esc/home

ANALYSIS OF RESPONDENTS’ OPINIONS AND ATTITUDES TOWARD THE SECURITY OF PAYMENT SYSTEMS[*]

Antonín Korauš[1], Miroslav Gombár[2], Pavel Kelemen[3], Jozef Polák[4]

[1] Academy of the Police Force in Bratislava, Sklabinská 1, 835 17 Bratislava 35, Slovak republic
[2,3,4] University of Prešov in Prešov, Faculty of Management, Konštantínova 16, 080 01 Prešov, Slovak Republic

E-mails:[1] antonín.koraus@minv.sk , [2]miroslav.gombar@unipo.sk , [3]kelemen.pavel@gmail.com ,[4] jozefpolak64@gmail.com

Received 15 February 2019; accepted 15 May 2019; published 30 June 2019

Abstract. The number of financial and cyber-attacks is increasing. The latter trend in financial and cyber security incidents is global and, as such it is being monitored globally. Cyber and financial statistical data and the growing number of certified information management systems show the practical importance of data security at the international level. The decisions to solve the data security problems are based on the technical point of view, protection motivation theory, and security standards. By analysing the security of payment system, this article aspires to aid in the development of secure systems. Its aim is to contribute to the knowledge and comprehension of the behaviour of payment systems users with special focus on the aspect of their security. The article analyses the opinions and attitudes of respondents toward the questions dealing with the security of payment systems and their behaviour when using payment cards. The analysis is carried out from the aspect of gender, age and education of respondents by using multidimensional statistical methods, namely factor analysis and analysis of dispersion.

Keywords: cyber-attack; security; payment systems; payment cards; security management; financial institution

Reference to this paper should be made as follows: Korauš, A.; Gombár, M.; Kelemen, P.; Polák, J. 2019. Analysis of respondents’ opinions and attitudes toward the security of payment systems, *Entrepreneurship and Sustainability Issues* 6(4): 1987-2002. http://doi.org/10.9770/jesi.2019.6.4(31)

JEL Classifications: F5, F52, K42, K24

Additional disciplines (besides the field of economics reflected in JEL classifications): information and communication; security, protection of people and property

---

[*] *The contribution is the result of Vega project no. 1/0194/19 “Research on process-oriented management of financial management focusing on detection of tax evasion in terms of international business”.*

http://doi.org/10.9770/jesi.2019.6.4(31)

1. Introduction

The question of effective economic security management has serious implications in the field of banking and other financial institutions in EU. It cannot be rationally resolved at the application level without forming a conceptual framework based on research and methodology. As a separate part of management supervision, the management of the economic security system should not prevent financial institutions from fulfilling their key functions and features. This can be possibly reached by integrating the process of ensuring the economic security into the mechanisms of general management of these institutions.

An average EU citizen believes that in “seeking to strengthen the European Union, the priority should be given primarily to the fight against crime”. According to many researchers, the majority of EU population is of the opinion that the most important public security problems are those of violent crimes, corruption, juvenile delinquency, and property crimes. It is their opinion that the police should pay utmost attention to the investigation of grave crimes, patrols in public places, and immediate response to received reports on crime. This indicates that the fight against crime has to get priority in ensuring public security (Eurostat database 2012).

Many leaders and decision makers in public and private organisations are realising that in addition to being a driver for innovation, productivity and growth, the digital environment also introduces uncertainties that can jeopardise economic and social prosperity. Digital security incidents can have far-reaching economic consequences for organisations, as for example in terms of disruption of operations, direct financial losses, and lawsuits, as well as in terms of loss of trust among their customers, employees, shareholders and partners. Although cases are still exceptional, while reflecting on the increasing reliance of industrial facilities, transportation systems and hospitals on ICT, one should also consider the possibility that digital security incidents can cause physical damage as well as human fatalities.

Finally, individuals are increasingly aware that there can be a downside to the many benefits they derive from the use of the digital environment. When their personal data are publicly disclosed or fall into the hands of unauthorised persons, these individuals face privacy breaches and potential physical, material and moral damage. They can be victims of financial fraud in relation to identity theft when their personal data or digital credentials are stolen from their own devices, compromised companies, or institutional information systems.

2. Theoretical background

The emergence of big data and cloud computing services, growth in Internet speed and importance of wired and wireless data transfer, increasing possibilities of hardware and software, increase in human communication functions being taken over by smart phones, and other emerging functions suggest that the significance of information technologies in our lives is growing (Štitilis et al. 2016; Štitilis et al. 2017; Fuschi, Tvaronavičienė 2014; Tvaronavičienė et al. 2016; Tvaronavičienė 2018; Limba, Šidlauskas 2018; Skvarciany et al. 2018; Okoro, Ekwueme, 2018; Korauš, et al. 2019a; Korauš et al. 2019b; Šišulák 2017). In today's technically advanced world, autonomous systems are rapidly gaining in popularity. The security risk is preferably assessed by means of quantitative systematic risk assessment methods, such as RM/RA CRAMM (Mullerova 2016, Mamojka, Mullerova 2016; Hajdu et al., 2014; Kordik and Kurilovská 2018) in combination with crime forecast maps (Mullerova, Mamojka 2017). In many cases of shoulder-surfing attack, the attackers rely on their ability to observe and remember the details they have observed (Tari et al. 2006; Máté, Kiss, 2017; Roth and Richter 2006; Mura, Vlacseková 2018; Vlacseková, Mura 2017). Cybernetic security issues, which are often perceived as synonymous with the safety of critical infrastructure (Dobrovič et al., 2017).

The increase in the number of sophisticated incidents results from many factors (Jančíková, Pasztorová 2018; Jančíková, Veselovská 2018). One of them is that the migration of criminal activities online has professionalised the attacks and increased the overall level of threat to digital security. From the occasional isolated robber to well-organised transnational groups, criminals have been demonstrating considerable technical innovation skills to commit financial, information and identity theft and blackmail individuals, businesses and governments (Aven, 2012; Ashford, 2013; Feshner, 2014).

Other factors include terrorists and their supporters who in conjunction with physical attacks, have also extended their actions to the digital environment by multiplying attacks on Internet sites. Although few cases have been extensively documented, industrial digital espionage has been mentioned as being on the rise (Jackson, 2014).

3. Material and methods

The present article aims to contribute to the knowledge and comprehension of the behaviour of payment card users with special focus on the aspect of their security. The article analyses the opinions and attitudes of respondents toward the questions dealing with the security of payment systems and their behaviour when using payment cards. The analysis is carried out from the aspect of gender, age and education of respondents by using multidimensional statistical methods, namely factor analysis and analysis of dispersion. The research as well as the selection of representative sample were carried out as follows:

- Time horizon of the survey: 20.02.2018 – 20.07.2018
- Representative sample: 1,012 respondents
- Number of questionnaires issued: 4,700
- Number of (completed) questionnaires collected: 3,288

The representative sample containing 1,012 respondents was selected by random number generator from fully completed questionnaires (3,288) in such a way that it would represent the population of Slovakia over 18 years of age from the aspect of their education, size of municipality, and region they live in, and occupation.

The analysed set is represented in five age categories in ranges 18-30 years, 31-40 years, 41-50 years, 51-60 years and over 60 years. These categories are composed of 206, 212, 192, 196 and 213 respondents, respectively, which represents 2.22%, 20.80%, 18.84%, 19.23%, and 20.90% of the analysed set, respectively. The research was conducted on 540 men (52,99%) and 479 women (47.01%). Geographically, the respondents were from the regions of Prešov, Košice, Banská Bystrica Žilina, Nitra, Trenčín, Trnava and Bratislava in amounts 134 (13.15%), 140 (13.74%), 117 (11.48%), 127 (12.46%), 127 (12.46%), 144 (14.13%), 112 (10.99%) and 118 (11.58%), respectively. The statistical set was composed of respondents with primary (n=300; 29.44%), secondary (n=438; 42.98%) and university education (n=281; 27.58%). The analysed sample is composed of respondents living in towns (n=518; 50.83%) and villages (n=501; 49.17%). The structure of respondents can be seen in Figures 1 – 4.

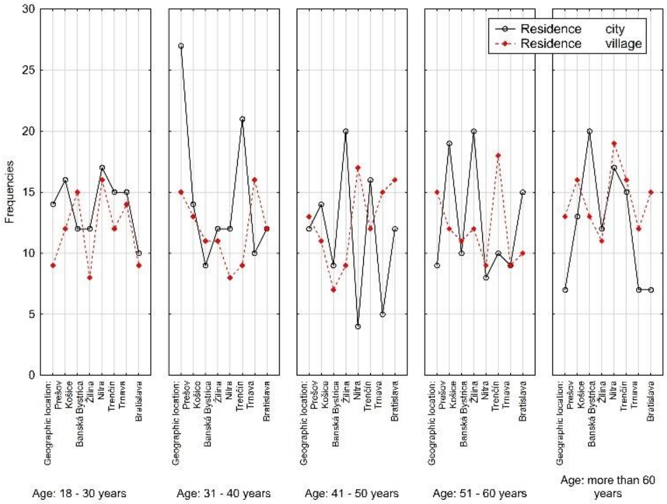

Figure 1. Structure of representative sample per residence, age and geographic region
Source: Own study

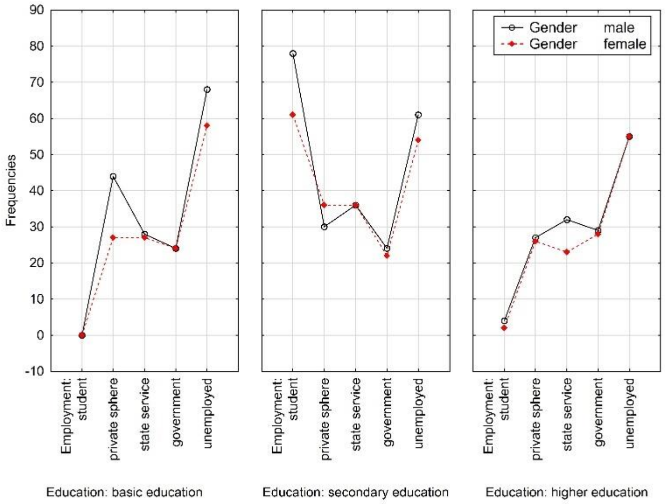

Figure 2. Structure of representative sample per education, gender and employment
Source: Own study

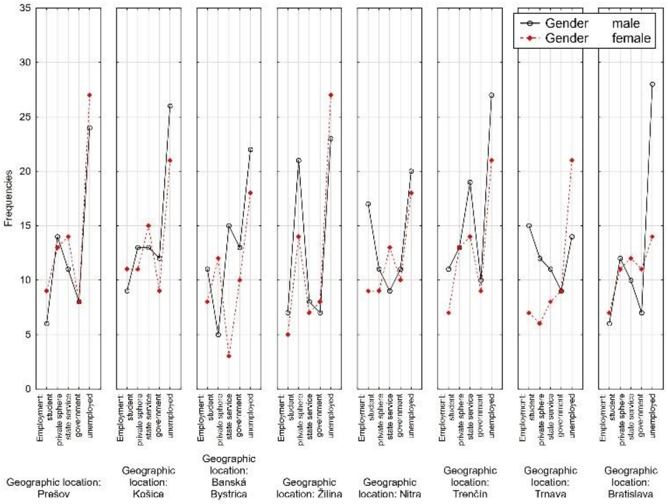

Figure 3. Structure of representative sample per geographic region, gender and employment
Source: Own study

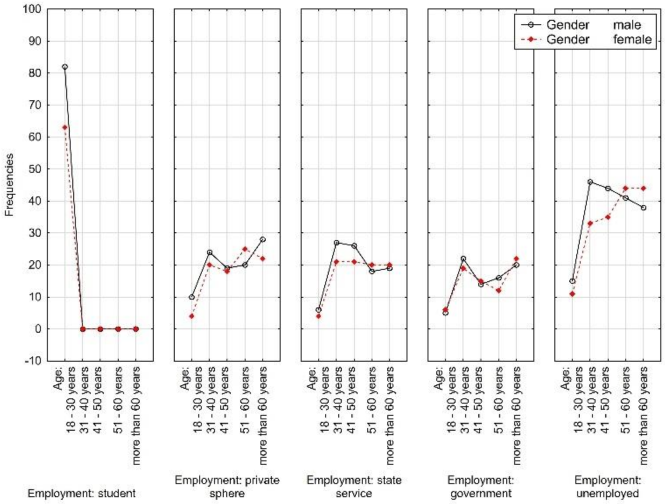

Figure 4. Structure of representative sample per employment, gender and age
Source: Own study

4. Results

The analysis of the behaviour of respondents when making a payment and their opinions on their security was based on answers to questions as follows:

- Q1 – Do you carry your payment card PIN code along with your payment card?
- Q2 – Have you ever changed your payment card PIN code?
- Q3 – Have you altered your payment card PIN code in a way that it would encode your date of birth?
- Q4 – Do you consider ATMs located at banks' premises safer for withdrawing your cash?

- Q5 – Do you have trust in the security of payment systems?
- Q6 – Do personal data represent information that needs to be most importantly protected?
- Q7 – Do you rely on the security measures of your bank in payment cards?
- Q8 – Are you sure that your bank takes proper care of your money?
- Q9 – Do you have any experience with a hacking attack or bank fraud?
- Q10 – Do you think that security measures taken to protect payment card data are continuously getting better?
- Q12 - How confident are you in the security of payment systems?
- Q13 – Do you think that the payment system carries elements of high security risks?
- Q18 – Does the enhanced security of new payment methods outweigh the cost of their implementation?
- Q19 – Does the enhanced customer convenience of new payment methods outweigh the cost of their implementation?
- Q20 - Why is it more challenging to secure payment card information?
- Q22 - How confident are you that customers can protect themselves when their personal information is lost or stolen?

The reliability of the research tool was judged by using the Cronbach's alfa coefficient. Its value was 0.81694. Based on the latter value, it is possible to state that it is not necessary to increase the value by removing any of variables. As the Cronbach alfa exceeds the value of 0.7, we can state that the research tool is reliable, and we can safely process the data.

The method is foremostly aimed at simplifying the description of group with mutual linear dependent signs, i.e. decomposing the source data matrix into structural and noise matrices. Each of main components represents a linear combination of original signs. Main components are ordered in line with their importance, i.e. with the decreasing dispersion (Tab. 1). This implies that a major portion of information on variability of original data is concentrated in the first main component and just as much information is concentrated in the last main component.

Table 1. Table of original values in the source matrix of researched set

Value number	**Eigenvalues of correlation matrix, and related statistics**			
	Eigenvalue	**% Total variance**	**Cumulative Eigenvalue**	**Cumulative %**
1	1,971471	12,32169	1,97147	12,3217
2	1,255233	7,84521	3,22670	20,1669
3	1,202084	7,51302	4,42879	27,6799
4	1,128291	7,05182	5,55708	34,7317
5	1,069369	6,68356	6,62645	41,4153
6	1,054192	6,58870	7,68064	48,0040
7	1,020088	6,37555	8,70073	54,3795

8	0,971202	6,07001	9,67193	60,4496
9	0,932597	5,82873	10,60453	66,2783
10	0,858880	5,36800	11,46341	71,6463
11	0,838353	5,23971	12,30176	76,8860
12	0,827242	5,17026	13,12900	82,0563
13	0,806948	5,04343	13,93595	87,0997
14	0,772271	4,82669	14,70822	91,9264
15	0,706586	4,41616	15,41481	96,3425
16	0,585192	3,65745	16,00000	100,0000

Source: Own study

The table of original values in source data matrix (Tab 1) shows that the concentrations of first, second, third, fourth, fifth, sixths and seventh main components are 12.32169 %, 7.84521 %, 7.51302 %, 7.05182 %, 6.68356 %, 6.5887 %, and 6.37555 % of variability of the original data, respectively. These seven main components, whose own number is larger than 1 concentrate within themselves 54.3795 % of variability of original data of the researched set. The diagram of the dispersion measures (Fig. 5) shows that the first main component divides the responses by vertical axis into two clusters, while at negative values of the component score of the first main component, the responses to 16 of posed questions (Q1 - Q10, Q12, Q13, Q18 – Q20 and Q22) are homogenous. As opposed to the latter, at positive values of component score of the first main component, the responses are more heterogenous. In combinations of second, third, fourth, fifth, sixth and seventh main components, the data are concentrated around the centre of the coordinate system and yield a homogenous structure in all directions.

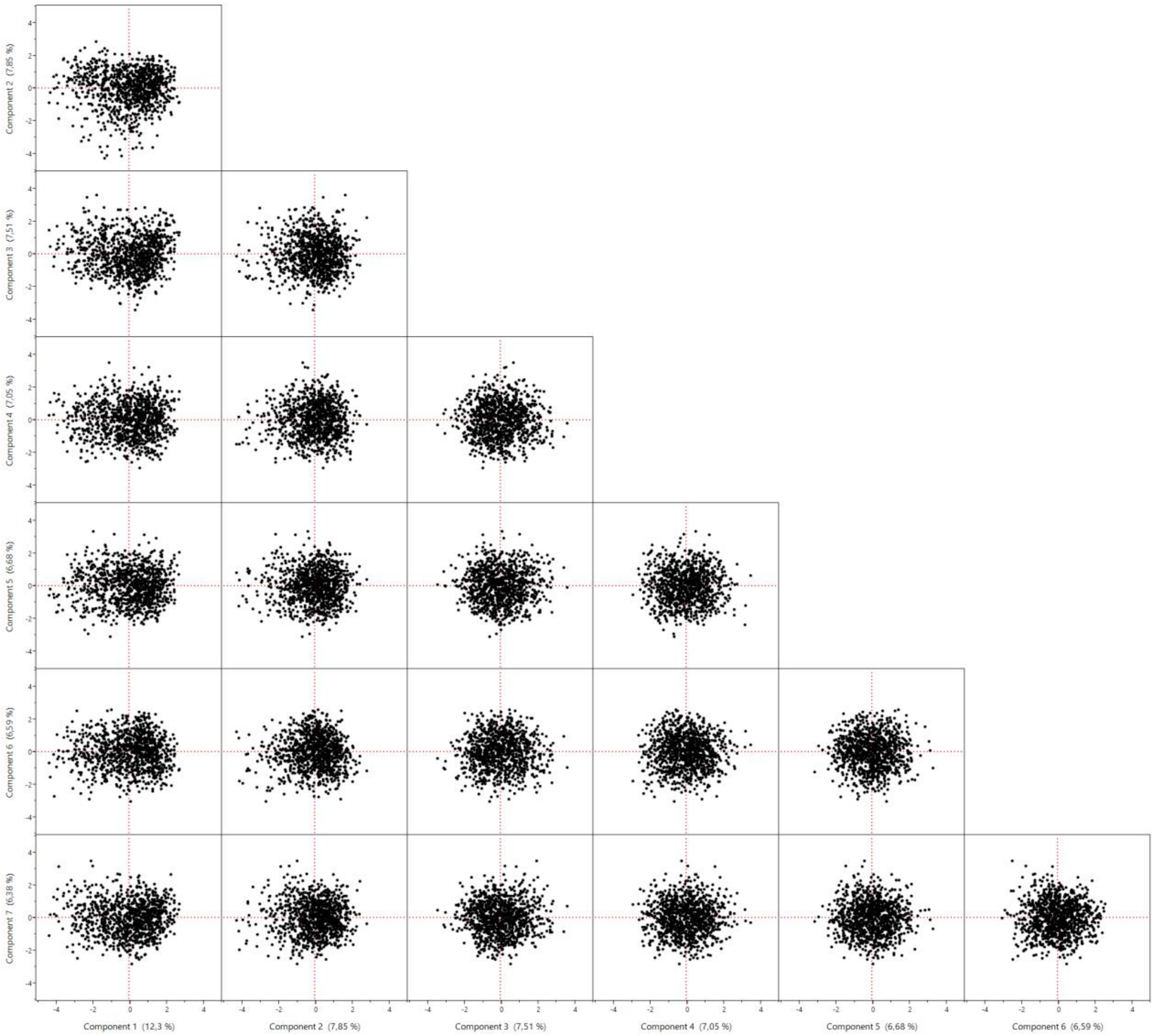

Figure 5. Dispersion diagram of component score
Source: Own study

The appropriate use of factor analysis is tested by Kaiser-Mayer-Olkin statistics and Bartlett's test of sphericity. KMO statistics represents an index which serves for comparing the size of experimental correlation coefficients against the size of partial correlation coefficients. When the sum of squares of partial correlation coefficients between all pairs of signs is small in comparison to the sum of squares of pair correlation coefficients, the measure of KMO statistics approaches the value of 1. Low values of KMO statistics indicate that the factor analysis of original signs would not be a good approach because the correlation between the pairs of signs cannot be explained by means of the rest of signs. In accord with the value of Keiser-Mayer-Olkin statistics (0.642) and definition by Kaiser, it is possible to state that based on the used research tool, the measure of correlation is good and the choice of factor analysis for security of payment system is justified. Bartlett's test of sphericity represents a statistical test of correlation between original signs. It tests the null statistic hypothesis H_0, namely whether "the correlation between the signs does not exist" , i.e. whether the correlation matrix is a unit matrix. The achieved level of significance of Bartlett's test of sphericity p= 0.000 is lower than the level of significance chosen by us (α = 5 %). Thus, we can reject the null hypothesis that the realisation of the selected correlation matrix with 16 considered variables is a unit matrix. Hence, to start off, we can state that the factor analysis is appropriate for the data dealing with security of payment system.

Table 2. Assumptions for the use of factor analysis (KMO statistics, Bartlett's test)

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		0,642
Bartlett's Test of Sphericity	Approx. Chi-Square	629,915
	df	120
	Sig.	0,000

Source: Own study

The first step to the interpretation of results of factor analysis is to analyse the factor matrix (Tab. 3) which serves for gaining the initial number of factors. The factor matrix contains factor loading for each sign, while in each factor, it represents the best linear combination of original signs while including the highest possible number of variability of signs. The first factor is always the most important because it represents the best linear relation found in original signs. The second factor represents the second best linear relation of original data, however it is restricted by a condition that it has to be orthogonal to the first factor. The factor loading explains the role of each original sign in defining the common factor. It is, in fact, a correlation coefficient between every original sign and factor.

Table 3. Factor loading

Variable	**Factor Loading (Varimax normalized) Extraction: Principal components**						
	Factor 1	**Factor 2**	**Factor 3**	**Factor 4**	**Factor 5**	**Factor 6**	**Factor 7**
Q1	0,667027	-0,056201	-0,009635	-0,057215	-0,047914	0,043137	-0,028946
Q2	-0,702289	-0,104631	0,149141	0,124769	-0,036834	0,127380	-0,138716
Q3	0,667834	0,008599	-0,008697	0,068546	0,022302	-0,218077	0,061900
Q4	0,030219	0,678758	-0,245063	0,044069	-0,098954	0,045068	0,133751
Q5	0,019901	-0,140903	0,650951	-0,000812	-0,066915	0,115440	0,296767
Q6	0,049937	-0,040089	0,062699	0,054951	0,009874	0,030645	0,783608
Q7	-0,014691	-0,126738	-0,064008	-0,134143	-0,056402	-0,732862	-0,095482
Q8	0,217457	0,031563	-0,055021	0,084674	0,078457	-0,654224	0,092631
Q9	-0,170928	0,049245	-0,095052	0,580158	0,203906	-0,203738	0,052174
Q10	-0,483641	0,224774	0,010966	-0,129255	-0,019166	-0,117729	0,352577
Q12	-0,202965	0,096779	0,555906	-0,202640	0,115733	0,055215	-0,145093
Q13	-0,062923	0,535860	0,004331	-0,038624	0,076363	0,080119	-0,338568
Q18	-0,031518	0,614785	0,422922	0,040299	0,008766	-0,002696	0,019843
Q19	0,055803	-0,088242	0,361737	0,298743	-0,592838	-0,237350	-0,194491
Q20	0,048449	-0,076490	0,168337	0,176893	0,804773	-0,122083	-0,100801
Q22	0,076839	0,000956	-0,051205	0,730203	-0,096729	0,236042	0,006834
Expl.Var	1,756082	1,254472	1,176141	1,104870	1,097575	1,238837	1,072751
Prp.Totl	0,109755	0,078404	0,073509	0,069054	0,068598	0,077427	0,067047

Source: Own study

The Table 3 makes it obvious that the first factor significantly correlates with components of research tool, namely with Q1 (Do you carry the payment card PIN code along with your payment card?), Q2 (Have you ever changed your payment card PIN code?), and Q3 (Have you altered your payment card PIN code in a way that it would encode your date of birth?). The values of factor loading reach the values of 60.7027 % and 66.7834 at components Q1 and Q3, respectively. The positive sign of factor loading reflects the indirect proportion, i.e. the evaluation of responses decreases on Likert scale with an increase in the number of respondents. Thus, in frame of the scale value, the responses stating “certainly not” or “no” are chosen. The factor loading of Q2 component of the research tool reaches the value of -70.2289. As it implies further from the analysis of Table 3, 44.4925 % of variability of Q1 component (“Do you carry the payment card PIN along with your payment card”), 49,321 % of variability of component Q2 (“Have you ever changed your payment card PIN?”) and 44, 6002 % of variability of component Q3 (Have you altered your payment card PIN code in a way that it would encode your date of birth? ”) are explained by the first mutual factor. The second mutual factor correlates with the component Q4 (Do you think that ATMs located at banks’ premises are safer for withdrawing your cash”), Q13 (“Do you think that the payment system carries elements of high security risks?”) and Q18 (“Does the enhanced security of new payment methods overweigh the cost of implementation?”) with the value of factor loading of 67.8758 % at component Q4, 53.586 % at component Q13, and 61.4785 % at component Q18. This implies that 46.0712 % of variability of component Q4, 28.7146 % of component Q13, and 37.7961% of variability of component Q18 are explained by the second mutual factor. The third mutual factor significantly correlates with the components Q5 (“Do you have trust in the security of payment systems?”) and Q12 (“How confident are you in the security of payment systems?”) with values of factor loading of 65.0954 % and 55.5906 %. From Table 3, it further implies that the variability values of 42.3737 % and 30.9031 % of Q5 and Q12 components, respectively, are explained by third mutual factor.

The fourth mutual factor correlates with components Q9 (“Do you have any experience with a hacking attack or bank fraud?”) and Q22 (“How confident are you that customers can protect themselves when their personal information is lost or stolen?”) with values of factor loading of 58.0158 % at Q9 component and 3.0203 % at Q22 component, which represents the values of 33.6583 % and 53.3196 % of variability of these components explained by the fourth mutual factor. The fifth mutual factor correlates with components Q19 (“Does the enhanced customer convenience of new payment methods outweigh the cost of implementation?”) and Q20 (“Why is it more challenging to secure payment card information?”) with factor loading values of -59.284 % and 80.4773 %, which represent the variability values explained by fifth mutual factor, namely those of 35.1457% and 64.766 % of Q19 and Q20 components, respectively. The sixth mutual factor correlates with components Q7 (“Do you rely on the security measures of your bank in payment cards?” and Q8 (“Are you sure that the bank takes proper care of your money?”). The factor loading values are -59.284 % and -65.422 % for Q7 and Q8 components of research tool, respectively. Both components yield a negative degree of correlation. The last, seventh extracted factor correlates with Q6 component (“Do personal data represent information that needs to be most importantly protected?”) with factor loading value of 78.3608 % which represents a variability of 61.4041 % of this component explained by seventh mutual factor. Aside from defining the basic mutual correlations, we have at the same time tested the practical significance of factors.

Based on the facts mentioned above, the factors of the main research objective, defined as a restriction of main identifiers of the security of payment systems and secure behaviour of respondents, can be postulated as follows:

- Factor 1 – PIN code
- Factor 2 – Awareness of security risks,
- Factor 3 – Knowledge of security elements,
- Factor 4 – Personal experience with fraud,
- Factor 5 – Enhancement of security of payment systems,

- Factor 6 – Trust in banks
- Factor 7 – Need of protecting the security elements.

The factor analysis focuses foremostly on parameters of the factor model. It may require estimations of mutual factors, which is referred to as factor score. The values of mutual factors in *n* selected observed objects or observations are not only a useful tool for diagnosing the data, but possibly also an important entry into further analyses. The factor score is not an estimation of parameters in common sense because it involves estimations of values of non-observed quantities. The estimations of factor score for a given object can be imagined as its coordinates in R-dimensional space.

Table 4. Coefficients of factor score

Variable	**Factor Score Coefficients Rotation: Varimax normalized Extraction: Principal components**						
	Factor 1	**Factor 2**	**Factor 3**	**Factor 4**	**Factor 5**	**Factor 6**	**Factor 7**
Q1	0,403974	-0,013833	0,052359	-0,061879	-0,025194	0,116074	-0,046696
Q2	-0,398755	-0,128143	0,058275	0,125695	-0,041488	0,025549	-0,119585
Q3	0,375695	0,057193	0,070984	0,054799	0,030542	-0,108248	0,042342
Q4	0,027875	0,548057	-0,210160	0,038413	-0,103424	0,005812	0,141195
Q5	0,072687	-0,104559	0,553875	0,010329	-0,027592	0,069398	0,255593
Q6	0,015465	-0,015685	0,039837	0,040412	0,018702	0,018291	0,727772
Q7	-0,102795	-0,061977	-0,027040	-0,115261	-0,078224	-0,606415	-0,076729
Q8	0,050911	0,078406	0,009138	0,079014	0,053975	-0,524822	0,092201
Q9	-0,137283	0,047838	-0,066609	0,528113	0,171820	-0,190067	0,054055
Q10	-0,301059	0,168865	-0,042920	-0,110880	-0,033603	-0,173483	0,350339
Q12	-0,045912	0,066089	0,467854	-0,163334	0,123199	-0,001508	-0,140003
Q13	0,011815	0,417752	0,011906	-0,024544	0,064394	0,035366	-0,305297
Q18	0,054389	0,502483	0,376989	0,055539	0,018987	-0,064813	0,019703
Q19	0,023964	-0,043568	0,321691	0,283831	-0,534320	-0,225482	-0,197507
Q20	0,049374	-0,056303	0,197145	0,166662	0,740724	-0,074662	-0,096994
Q22	0,055867	-0,000993	-0,032630	0,656919	-0,080331	0,198365	-0,007713

Source: Own study

Graphical representation of the relations between individual components of research tool and extracted factors 1 and 2 are shown in Figure 6. The latter figure makes it obvious that Q1 and Q3 components correlate positively with Factor 1, while the Q2 component correlates negatively with the latter factor. Q4, Q13 and Q18 components strongly and positively correlate with Factor 2 while their relation to Factor 1 is moving in a narrow interval from -0.1 to +0.1. In a particular manner, Q10 component also correlates with Factor 1, however the value of factor loading in relation to Factor 1 is lower than 0.5.

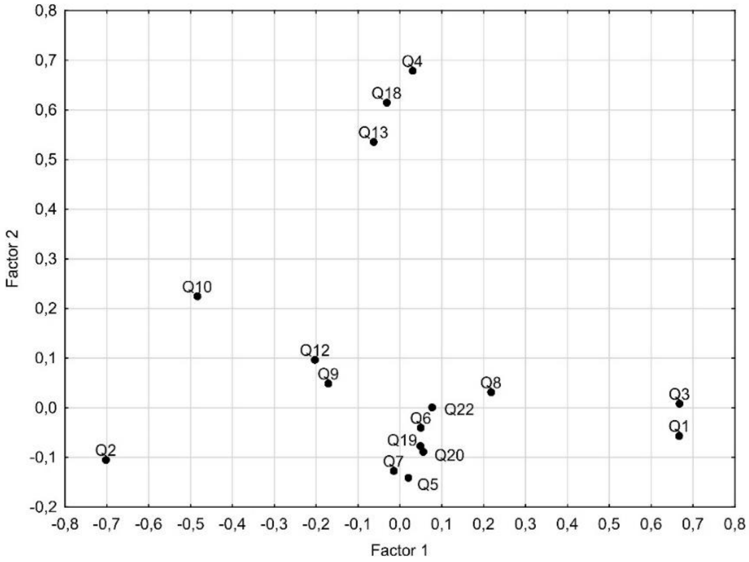

Figure 6. Graph of dependencies of the components of research tool on factors 1 and 2
Source: Own study

The graph of factor score for individual extracted factors is shown in Figure 7. For better illustration and transparency, always the first ten respondents of selected groups are depicted.

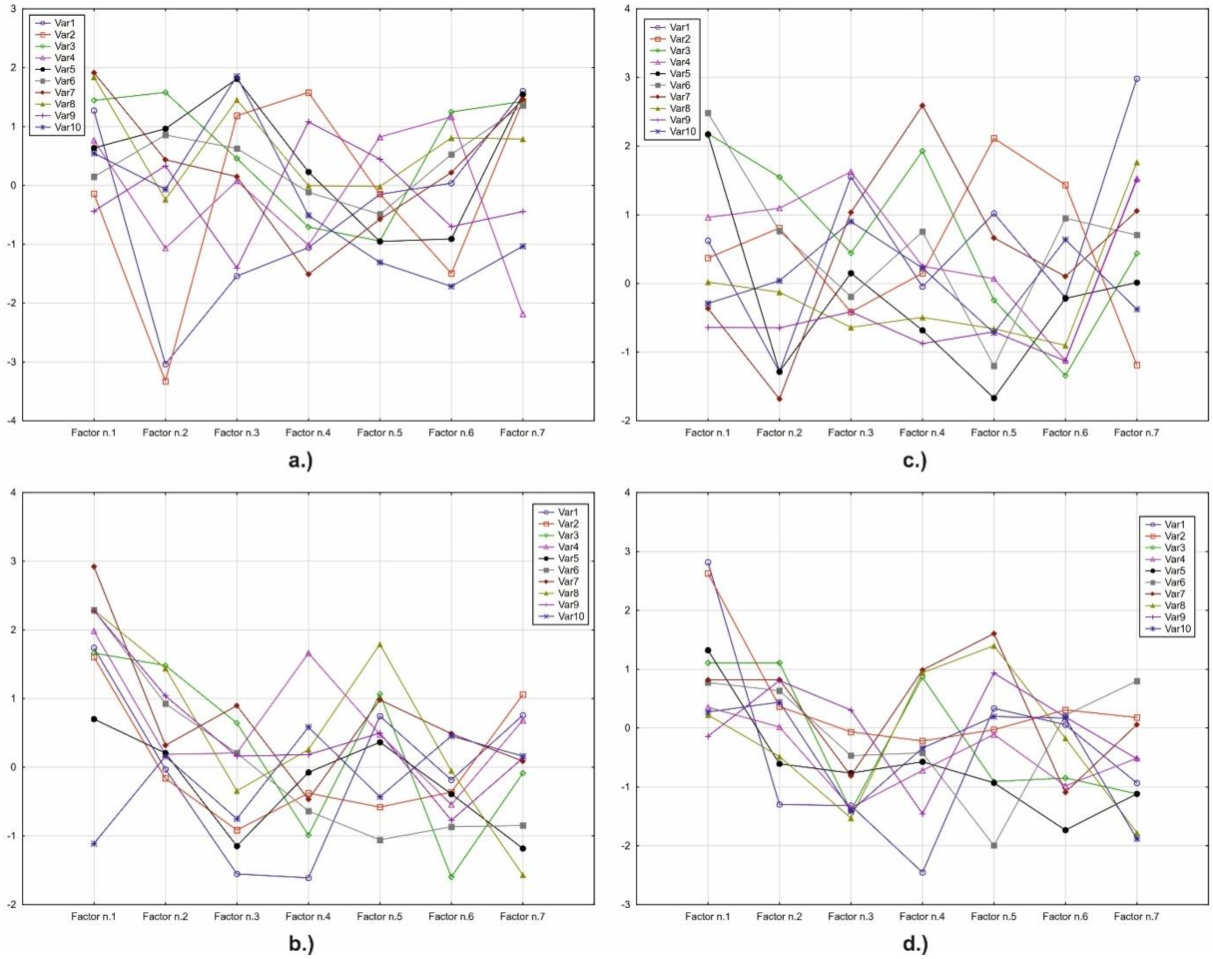

Figure 7. Graph of factor score for individual extracted factors
a) man, 31-4 years of age, secondary education; b) man over 60 years of age, secondary education; c) woman over 60 years of age, secondary education

Source: Own study

The Figure 7 depicts the factor score for the first ten respondents. It shows that at Factor 1 (defined as PIN code and observed to be correlating with Q1, Q2 and Q3 of the questionnaire), we see a positive perception in both women and men at 31-40 years of age, which means that the latter respondents attach importance to the rules for using the PIN code. A similar trend in Factor 1 can be seen also in men and women over 60 years of age, however this age category yields higher absolute values of the factor score. As to Factor 2 (defined as awareness of security risks), men and women at age of 31-40 years respond similarly on both poles, even though in both groups particular extreme values can be found. In the category over 60 years of age, the respondents of both genders are leaning towards positive values of the factor score. The presented analyses enable us to reason that the responses relating to the security of payment systems differ in the categories of 31-40 years of age and over 60 years of age, however an obviously similar trend in the distribution of factor score can be seen when comparing men and women. This means that the opinion about the security of payment systems is not influenced by gender.

Conclusions

It is of importance to state that a conclusion laid out in greater detail would require the questionnaire to be further analysed while the conclusions implying from age differences as well as gender similarities in respondents' opinions about the security of payment systems would have to be further statistically tested.

The professionalisation of threat sources has led to increased sophistication of offensive technical tools, some of which are automated and deployed on a large scale for maximum impact, while others are carefully tailored to specific valuable targets and to evade detection and attribution. Malicious codes are used to stealthily penetrate information systems, monitor them and then extract confidential data such as trade or political secrets over extensive periods of time (called Advanced Persistent Threat, "APT"). Botnets comprising thousands to millions of infected computers and devices can be rented to perform denial of service attacks in order to blackmail their owner or to express discontent. Social engineering techniques are also very common, for example through emails that look legitimate but enable the attacker to steal credentials or penetrate the user's system ("phishing").

Financial public and private sector organisations are progressively recognising the scale of the challenge and adjusting their practices. In particular, an increasing number of top senior executives in large financial firms understand that a purely technical approach is insufficient to manage digital security risk. However, many public and private organisations, and in particular small and medium enterprises (SMEs), are not yet ready to manage digital security risk from an economic perspective and still consider this issue as mainly technical. Finally, the increasing number of massive data breaches exposing personal data and leading in some cases to financial fraud and identity theft raises concerns among individuals who are often left on their own, without the means, knowledge and skills to effectively manage this risk.

References

Ashford, W. (2013), Targeted cyber espionage on the increase, McAfee warns, www.computerweekly.com/news/2240185167/Targeted-cyber-espionage-onthe-increase-McAfee-warns.

Aven, T. (2012). The risk concept - historical and recent development trends, *Reliability Engineering & System Safety* 99: 33–44. http://dx.doi.org/10.1016/j.ress.2011.11.006.

Dobrovič, J., Gombár, M., Benková, E. (2017). Sustainable development activities aimed at combating tax evasion in Slovakia. *Journal of Security and Sustainability Issues,* 6(4): 761-772. https://doi.org/10.9770/jssi.2017.6.4(19)

Eurostat database (2012). Economy and finance. Retrieved from http://epp.eurostat.ec.europa.eu/portal/page/portal/eurostat/home/

Fechner, B. (2014), Les entreprises françaises face au défi de l'espionnage industriel, http://lexpansion.lexpress.fr/actualite-economique/les-entreprisesfrancaises-peuvent-elles-relever-le-defi-de-l-espionnage-industriel_1633978.

Fuschi, D., Tvaronavičienė, M. (2014). Sustainable development, Big Data and supervisory control: service quality in banking sector, *Journal of Security and Sustainability Issues* 3(3): 5-14. http://dx.doi.org/10.9770/jssi.2014.3.3(1)

Hajdu, Z., Andrejkovič, M., & Mura, L. (2014). Utilizing experiments designed results during error identification and improvement of business processes, *Acta Polytechnica Hungarica* 11(2): 149-166. https://doi.org/10.12700/APH.11.02.2014.02.9

Jackson, W. (2014), "Cyber Espionage Incidents Triple: Verizon Report", www.informationweek.com/government/cybersecurity/cyber-espionage-incidentstriple-verizon-report/d/d-id/1204612

Jančíková, E., Veselovská, S. (2018). The new Technologies and the Fight Against Money Laundering and the Terrorism Financing. In *2nd International Scientific Conference - EMAN 2018 - Economics and Management: How to Cope With Disrupted Times*, Ljubljana - Slovenia, March 22, 2018, ISBN 978-86-80194-11-0. https://doi.org/10.31410/EMAN.2018.334

Jančíková, E., Pásztorová, J. (2018). Strengthened EU Rules to Tackle Money Laundering and Terrorism Financing and their Implementation in Slovak Republic. In Staníčková, M., L. Melecký, E. Kovářová and K. Dvoroková (eds.). *Proceedings of the 4 th International Conference on European Integration 2018* . Ostrava: VŠB - Technical University of Ostrava, 2018, pp. 528-536. ISBN 978-80-248-4169-4. ISSN 2571-029X.

Korauš, A.; Dobrovič, J.; Polák, J.; Backa, S. (2019a). Security aspects: protection of people in connection with the use of personal identification numbers, *Journal of Security and Sustainability Issues* 8(3): 319-330. http://doi.org/10.9770/jssi.2019.8.3(3)

Korauš, A.; Gombár, M.; Kelemen, P.; Backa, S. (2019b). Using quantitative methods to identify insecurity due to unusual business operations, *Entrepreneurship and Sustainability Issues* 6(3): 1101-1012. http://doi.org/10.9770/jesi.2019.6.3(3)

Kordík, M.; Kurilovská, L.; Intra Group Compliance Agreement as a tool to manage the risks in the daughter companies, *Enterpreneurship and Sustainability Issues* n. 4/2018, ISSN (online) 2345-0282 p.1008-1019, https://doi.org/10.9770/jesi.2018.5.4(21)

Limba, T.; & Šidlauskas, A. (2018). Secure personal data administration in the social networks: the case of voluntary sharing of personal data on the Facebook, *Entrepreneurship and Sustainability Issues* 5(3): 528-541. https://doi.org/10.9770/jesi.2018.5.3(9)

Mamojka, M.; & Müllerová, J. (2016). New methodology for crisis management RM/RA CRAMM and its legal frame. In: Production management and engineering sciences. - Leiden: CRC Press/Balkema, 2016. pp 185-190. ISBN 978-1-138-02856-2.

Máté, D., Kiss, Z. (2017). An assessment of financial knowledge in higher education. Acta Oeconomica Universitatis Selye 6 (1): 83 – 98. ISSN 1338-6581

Mura, L.; & Vlacseková, D. (2018). Motivation of public employees: case study of Slovak teaching and professional staff. *Administratie si Management Public*, (31): 67-80. https://doi.org/10.24818/amp/2018.31-05

Müllerová, J. (2016). RM/RA CRAMM as a new risk management method for prevention of ecology disasters, 16th International Multidisciplinary Scientific GeoConference SGEM 2016, SGEM2016 Conference Proceedings, June 28 - July 6, Book5 Vol. 1, pp. 607-612. ISBN 978-619-7105-65-0 / ISSN 1314-2704

Müllerová, J.; & Mamojka, M. (2017). Legal possibilities of the rescue forces during the emergency event. In: SGEM2017 Conference Proceedings, 29 June - 5 July, 17(51): 605-612, ISBN 978-619-7408-08-9 / ISSN 1314-2704. DOI: 10.5593/sgem2017/51/S20.079

Okoro, E. G., Ekwueme, C. M. (2018). Determinants of bank performance in Nigeria: the dynamics of internality and externality measures. *Acta Oeconomica Universitatis Selye* 7(1): 108 – 120. ISSN 1338-6581

Roth V.; & Richter, K. (2006). “How to Fend off Shoulder Surfing,” Journal of Banking and Finance, 30(6): 1727-1751. ISBN:1-58113-961-6 https://doi.org/10.1145/1030083.1030116

Skvarciany, V., Jurevičienė, D., Iljins, J., & Gaile-Sarkane, E. (2018). Factors influencing a bank’s competitive ability: the case of Lithuania and Latvia. *Oeconomia Copernicana*, 9(1): 7-28. https://doi.org/10.24136/oc.2018.001

Šišulák, S. (2017). Userfocus - tool for criminality control of social networks at both the local and international level, *Entrepreneurship and Sustainability Issues* 5(2): 297-314. https://doi.org/10.9770/jesi.2017.5.2(10)

Štitilis, D.; Pakutinskas, P.; Laurinaitis, M.; & Malinauskaitė, I. (2017). A model for the national cyber security strategy. The Lithuanian case. *Journal of Security and Sustainability Issues* 6(3): 357-372. https://doi.org/10.9770/jssi.2017.6.3(3)

Štitilis, D.; Pakutinskas, P.; Kinis, U.; & Malinauskaitė, I. (2016) Concepts and principles of cyber security strategies, *Journal of Security and Sustainability Issues* 6(2): 197-210. https://doi.org/10.9770/jssi.2016.6.2(1)

Tari F., Ozok A., & Holden S., (2006). “A Comparison of Perceived and Real Shoulder-Surfing Risks between Alphanumeric and Graphical Passwords,” In Proceedings of the Second Symposium on Usable Privacy and Security, Pittsburgh, pp. 56-66. ISBN: 1-59593-448-0 doi>10.1145/1143120.1143128

Tvaronavičienė, M. (2018). Towards sustainable and secure development: energy efficiency peculiarities in transport sector, *Journal of Security and Sustainability Issues* 7(4): 719-725. https://doi.org/10.9770/jssi.2018.7.4(9)

Tvaronavičienė, A., Žemaitaitienė, G., & Bilevičienė, T. (2016). Ecosystem for sustainable entrepreneurship: towards smart public procurement review procedures. *Entrepreneurship and Sustainability Issues* 4(1): 39-52. http://dx.doi.org/10.9770/jesi.2016.4.1(4)

Vlacseková, D.; & Mura, L. (2017). Effect of motivational tools on employee satisfaction in small and medium enterprises. *Oeconomia Copernicana*, 8(1): 111-130. https://doi.org/10.24136/oc.v8i1.8

Aknowledgements

The contribution is the result of Vega project no. 1/0194/19 "Research on process-oriented management of financial management focusing on detection of tax evasion in terms of international business".

Short biographical note about the contributors at the end of the article (name, surname, academic title and scientific degree, duties, research interests):

Assoc. Prof. Ing. Antonín KORAUŠ, PhD., LL.M., MBA is an associate professor at Academy of the Police Force in Bratislava, Slovak Republic. Research interests: economy security, finance security, cyber security, energy security, finance, banking, management, AML, economic frauds, financial frauds, marketing, sustainability.
ORCID ID: https://orcid.org/0000-0003-2384-9106

Assoc. Prof. Ing. Miroslav GOMBÁR, PhD**.** is an associate professor in the Department of Management, Faculty of Management at the University of Prešov in Prešov since 2016. Since 2016, he works as head of the Department of Management, and teaches school subjects: statistics, management, operations management, and logistics.
ORCID ID: https://orcid.org/0000-0002-8383-7820

Mgr. Pavel KELEMEN, Ph. D. Candidate at the Faculty of Management at the University of Prešov in Prešov, Slovak Republic
ORCID ID: https://orcid.org/0000-0001-7563-3142

Ing. Jozef POLÁK, Ph.D. Candidate at the Faculty of Management at the University of Prešov in Prešov, Slovak Republic
ORCID ID: https://orcid.org/0000-0003-4733-0851

Register for an ORCID ID:
https://orcid.org/register