JOURNAL OF SECURITY AND SUSTAINABILITY ISSUES
ISSN 2029-7017 print/ISSN 2029-7025 online
2019 June Volume 8 Number 4
http://doi.org/10.9770/jssi.2019.8.4(12)

Scopus®

AWARENESS OF SECURITY RISKS ASSOCIATED WITH PAYMENT SYSTEMS ANALYSED BY THE METHODS OF MULTIDIMENSIONAL STATISTICS

Antonín Korauš[1], Miroslav Gombár[2], Pavel Kelemen[3], Stanislav Backa[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]stanislav.backa@gmail.com

Received 15 November 2018; accepted 25 April 2019; published 30 June 2019

Abstract. At the heart of any banking system, there is the provision of payments. Payments can be made via fiat or crypto currencies, bank credit or deposits, or fund transfers on the books of non-bank payment providers. When using payment systems, security and protection of people and property are extremely important, especially in relation to cyberterrorism. The purpose of cybercrime is to gain material benefit using IT systems, while its targets can be both business and political actors. The focus of this article is on a profound analysis of extracted factors which would be necessary for achieving a comprehensive understanding and depiction of users' behaviours and risks in the field of security of payment instruments as well as technologies aimed at improving intermediated retail payment transactions.

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.; Backa. 2019. Awareness of security risks associated with payment systems analyzed by the methods of multidimensional statistics, *Journal of Security and Sustainability Issues* 8(4): 687–703. http://doi.org/10.9770/jssi.2019.8.4(12)

JEL Classifications: E42, G21, G23, L81

Additional discipline: information and communication; security, protection of people and property

1. Introduction

Payment innovations improve the payment system in at least four ways (Chakravorti and Kobor 2005). Firstly, they may improve the existing clearing and settlement processes required to convert payments into cash or bank deposits. For example, the ability of a check recipient to deposit checks via her mobile phone by taking a picture and uploading that image to her financial institution improves the processing of checks. In addition, financial institutions without widespread physical presence are able to better compete with those that have extensive branch networks for demand deposit (checking) accounts with remote check deposits. The remote capture technology is generally being offered by financial institutions but needs not be (Federal Reserve Bank of Chicago 2006).

Secondly, payment innovations may provide access to existing payment networks for buyers and sellers that have not traditionally had access. For example, PayPal allowed individuals to indirectly accept card payments in an online environment (Chakravorti, 2016).

Thirdly, large retail and social networks are well-positioned to make future payment innovations especially those that leverage extensive network connectivity to promote greater sales which might otherwise be lost (Chakravorti, 2016).

Fourthly, new payment systems may be created from scratch because the existing infrastructure is outdated and may prevent future innovation. New payment systems are difficult to build because building a new infrastructure is costly and usually has to occur alongside the existing infrastructure with buy-in of many stakeholders (Chakravorti, 2016).

2. Theoretical background

Cybersecurity is a continuous planning of processes with consideration to the political, legal, economic, educational, and technical measures with the efforts to reduce the risks associated with the cyberspace (Bányász, 2018; Limba et al. 2017; Tvaronavičienė 2018; Davidavičienė et al. 2019; Batkovskiy et al. 2019). Cybersecurity is one of the main concerns of organization especially with the increase in the sophistication of cyberthreats and attacks. These vulnerabilities have led to the exploitation of the cybersecurity infrastructure by cybercriminals. The activities of cybercriminals create issues of irrevocable funds transfer, monetary loss, loss of data, security breach, exposure and theft of customer's personal information, and infringing on intellectual property, thus, leading to significant financial brand equity loss and investor/customer confidence loss in these financial institutions (Christiansen and Piekarz, 2019; Okanazu, 2018; Mura et al., 2015). Cybernetic security issues, which are often perceived as synonymous with the safety of critical infrastructure (eg Dobrovič et al., 2017; Veselovska et al., 2017; Korauš et al., 2019a; Šišulák 2017;), need to be emphasized.

Cybersecurity comprises technologies, systems, processes, standards, regulatory frameworks that financial institutions in euro area countries utilize to prevent any form of intrusion into the network of the organization (Schwab, 2018). Therefore, cybersecurity is an integral part of financial institutions. It thrives on e-commerce platform as a modern-day means of business transaction leveraging on the Internet and mobile banking (Abbe, 2018; Okoro and Ekwueme, 2018). In view of the jeopardizing effect on financial institutions in euro area countries, cybersecurity serves to protect these institutions (Thapliyal et al., 2017). Due to the complexities of the cyber domain, there is a lack of a sophisticated cybersecurity framework to protect the network and other systems from attack (Korauš et al., 2019b; Horecký, 2018).

The issue of cybersecurity is the primary concern of financial institutions in euro area countries as this threatens the success of the institutions (Bayuk, et al. 2012) due to the total dependence on advancements in information technology (Radu, 2002). With information technology, the financial institutions in euro area countries began e-commerce through the development of the Internet, networks, technological tools such as computers and computer systems, development of applications and software for mobile e-commerce apps, as well as development of codes, thereby placing the institutions at a competitive edge (Ras, 2016; Hajdu et al., 2014).

As a result of the use of Internet and due to vulnerabilities, that existed in the network, the growth in the economy brought about an increase in cybercrimes (Jančíková, Pasztorová 2018; Jančíková, Veselovská 2018). These vulnerabilities made it easy to hack and perpetrate crimes such as illegal transfer of funds, identity thefts, frauds, and much more (Marty 2013). Awareness of security risks research Kordik and Kurilovská (2018), reliable risk assessment method RM/RA CRAMM applicable for a crime risk assessment was described by Mamojka and Mullerova (2017) and its legal questions by Mullerova and Mamojka (2017).

3. Material and methods

The present article deals with the results of research and subsequent analysis. It aims to contribute to the knowledge and comprehension of the behaviour of payment card users with a 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.

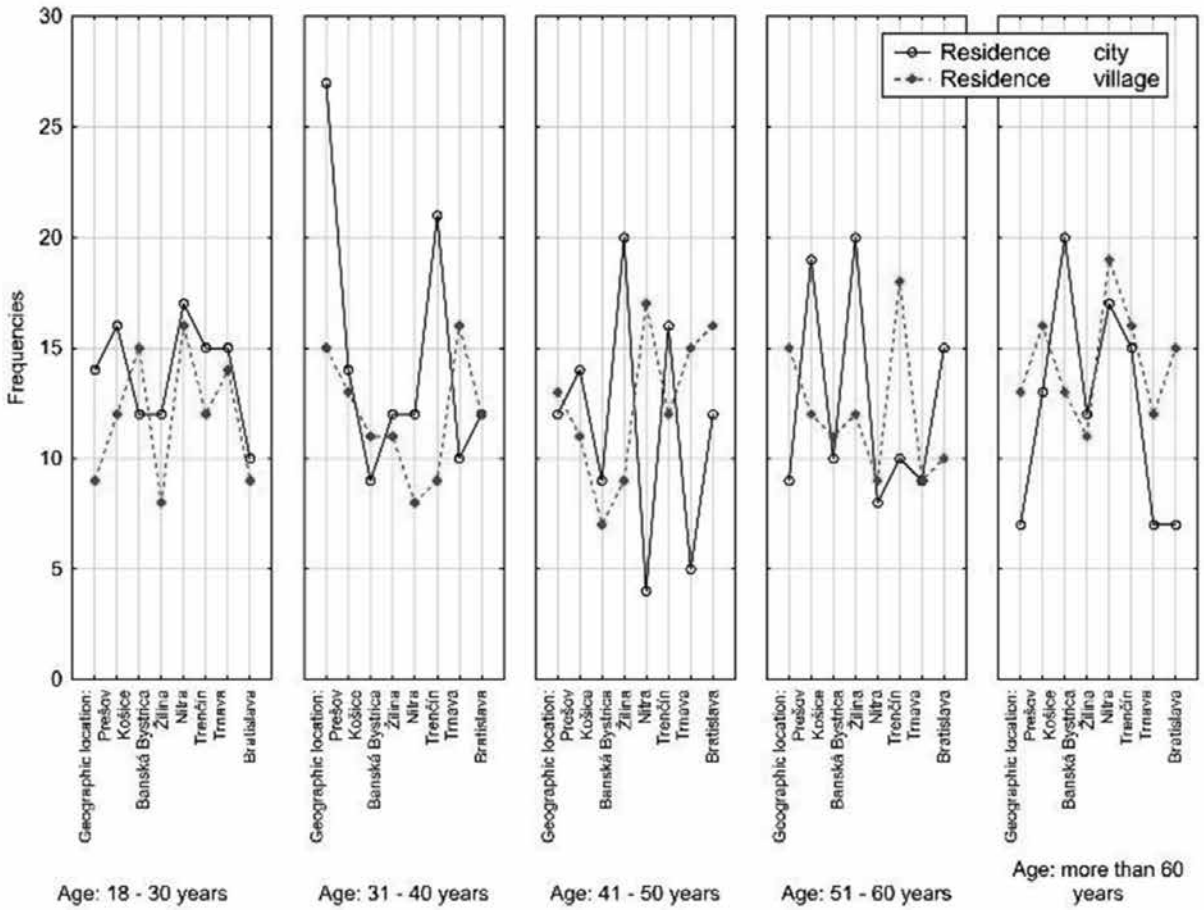

Figure. 1. Structure of representative sample per residence, age and geographic region

Source: Own study

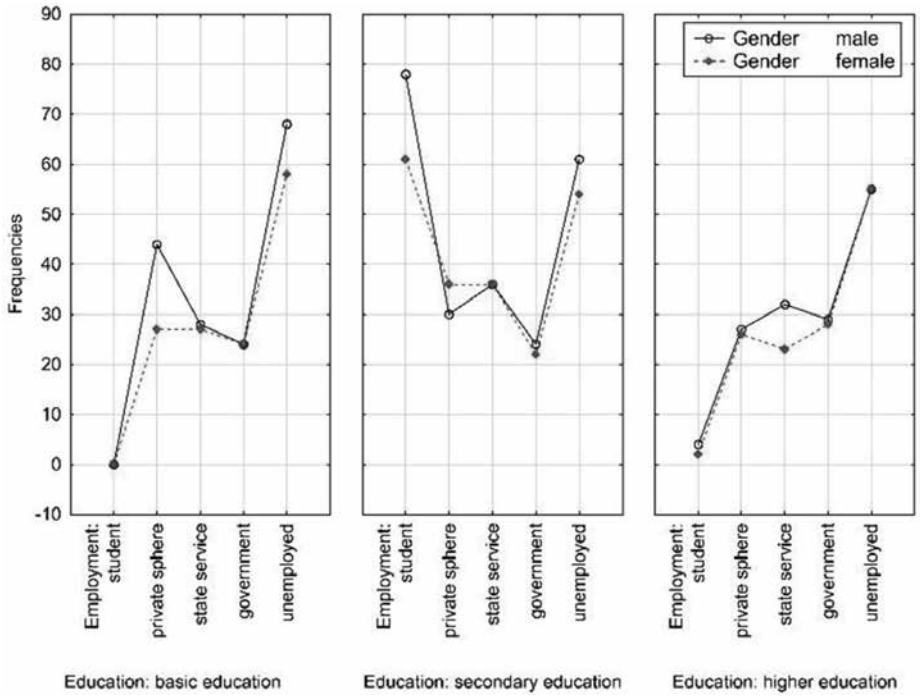

Figure 2. Structure of representative sample per education, gender and employment

Source: Own Study

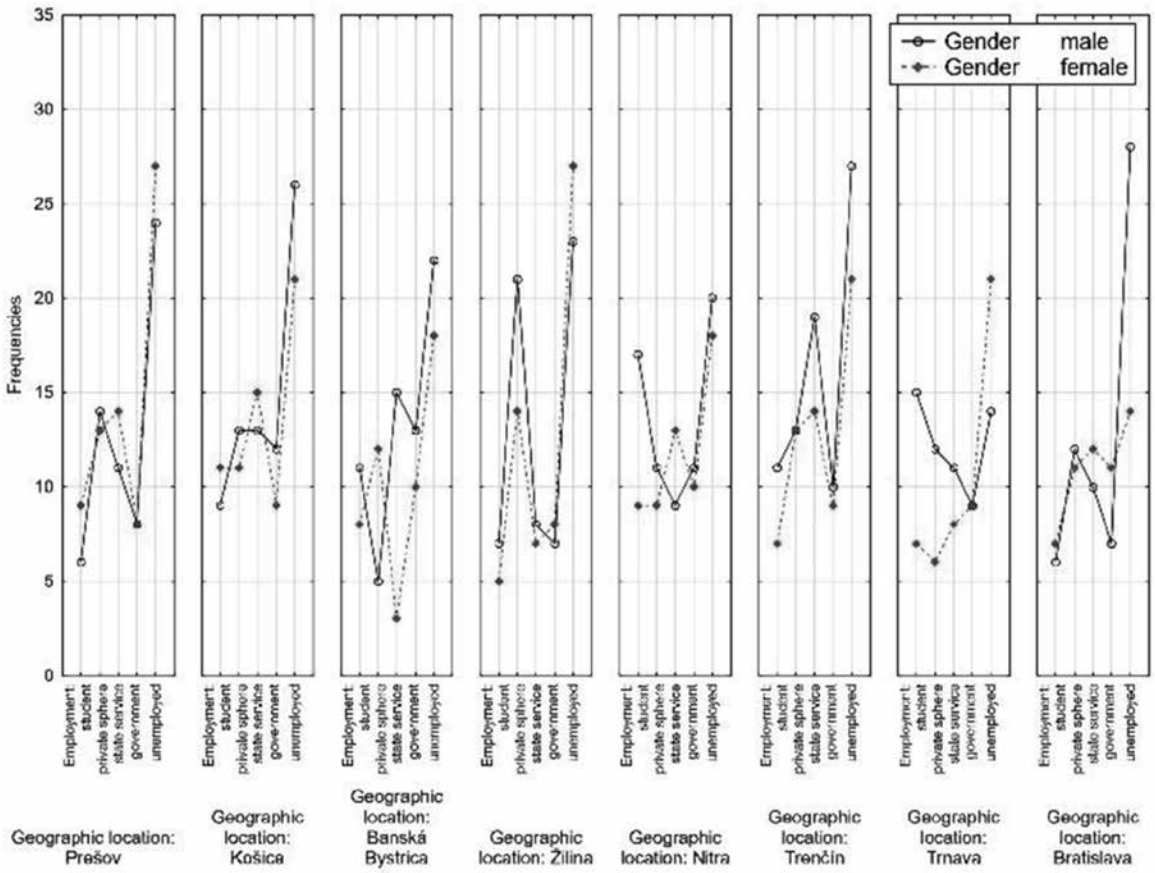

Figure 3. Structure of representative sample per geographic region, gender and employment

Source: Own study

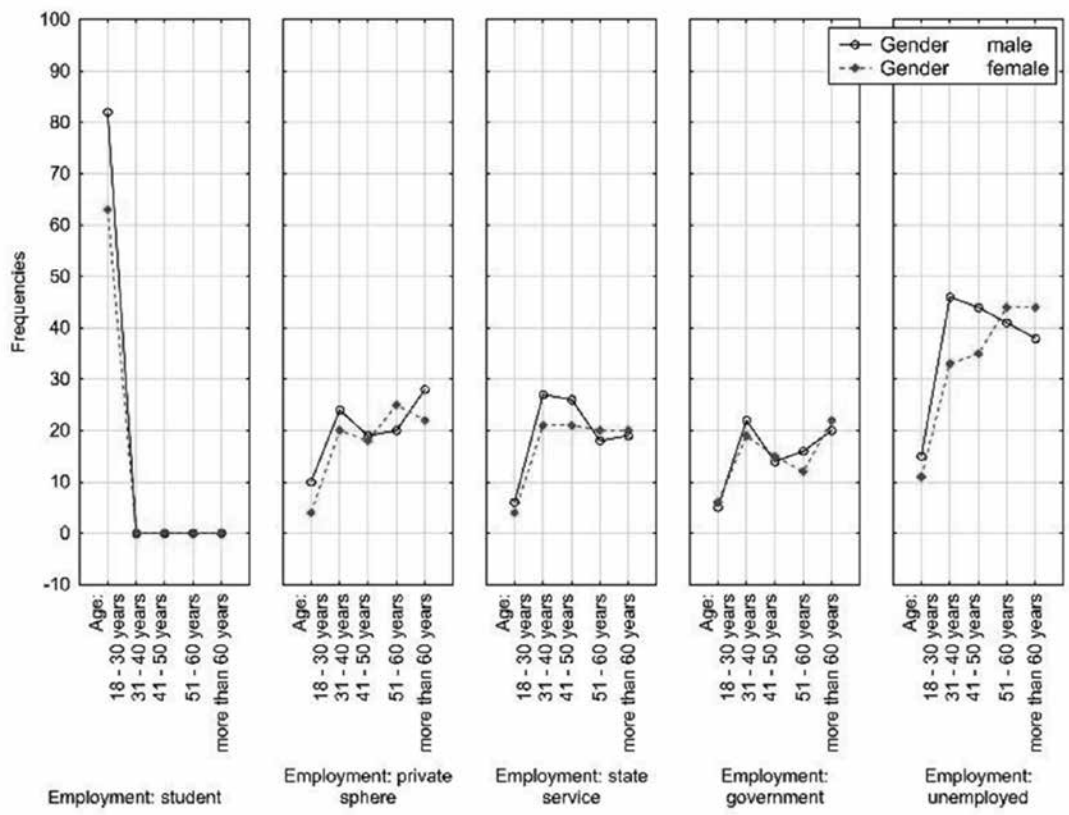

Figure 4. Structure of representative sample per employment, gender and age

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

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 center of the coordinate system and yield a homogenous structure in all directions.

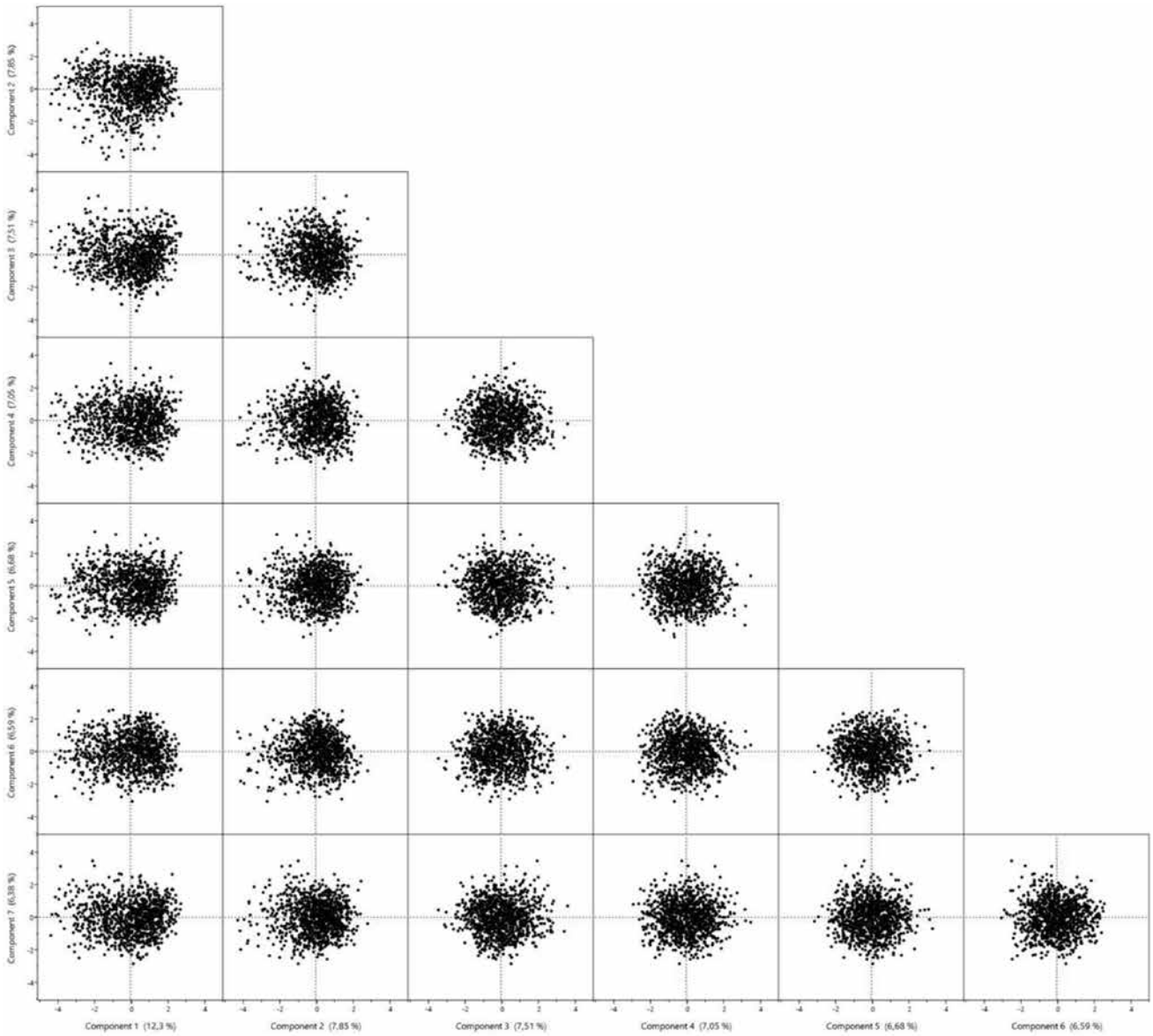

Figure 5. Dispersion diagram of component score

Source: Own study

The appropriate use of factor analysis is tested by Kaiser-Mayer-Olkin (KMO) 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 ($\alpha = 5$ %). Thus, we can reject the null hypothesis that the realization 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 your 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 your payment card PIN code along with your

payment card"), 49,321 % of variability of component Q2 ("Have you ever changed your payment card PIN code?") 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 consider ATMs located at banks' premises 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 their 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 your 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 tested also 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 behavior 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

In line with the defined goals of research, the subsequent section deals with the analysis of respondents' opinions or attitudes represented by factor score in relation to extracted identifiers, factors of payment system security by means of Fisher's ANOVA. Within the analysis, we shall be considering only the impact of significant independent variables or that of their interactions on the value of respective factor at the selected level of significance $\alpha = 0.05$.

ANOVA is an acronym standing for analysis of variance. ANOVA serves for comparing various sources or characteristics of various classes. These sources are referred to as factors and can contain several various levels. The goal is to decide whether the mean value of the measured quantity differs for various factors. This is demonstrated by testing the hypothesis on impact of factor on the mean value. In this case, the zero hypothesis states that the mean values of tested groups do not differ significantly.

Table 5. ANOVA for Factor 2 (Awareness of security risks)

Effect	Univariate Tests of Significance for Factor n.2 Sigma-restricted parameterization Effective hypothesis decomposition				
	SS	**Degr. of Freedom**	**MS**	**F**	**p**
Intercept	0,0142	1	0,01416	0,01508	0,902302
Age	16,5457	4	4,13643	4,40494	0,001557
Gender	0,4656	1	0,46560	0,49583	0,481506
Education	29,5490	2	14,77452	15,73358	0,000000
Age*Gender	2,6165	4	0,65413	0,69659	0,594382
Age*Education	20,4973	8	2,56216	2,72848	0,005595
Gender*Education	1,7138	2	0,85689	0,91252	0,401850
Age*Gender*Education	7,0529	8	0,88161	0,93884	0,483248
Error	928,7144	989	0,93904		

Source: Own study

The Table 5 shows that a change in Factor 2 (Awareness of security risks) expressed by factor score is significantly influenced by the age of respondents, their education, and mutual interaction of age and education, namely at the level of significance of α = 5 %. When the factor score is, as a result of factor analysis, considered a measure of consent, attitude or importance for the respondent, while a positive or negative number represents a positive perception and importance or negative attitude and unimportance of the given factor for respondents, respectively, then we can state that the average value of factor score for the category of 18 – 30 years of age represents a value of 0.4581±0.140016. This can be interpreted as an indifferent attitude to the problem of awareness of security risks for the observed age category of respondents. The category of 31-40 years of age reaches the factor score of -0.171639±0.158674.

Hence, according to the research results and subsequent analysis, the observed age category is not aware of security risks and this question is on the negative border of the bipolar scale. The category of 41-50 years of age reaches the average value of -0.15118±0.147917 of factor score, which indicates an equally negative attitude and approach to the awareness of security risks in payment instruments, especially payment cards. A higher importance represented by positive values of average factor score can be found in category of 51-60 years pf age, where it reaches the value of +0.089848±0.126367, and in category over 60 years of age, where it reaches the value of 0.189848±0.106776. The average values of factor score in individual age categories for the second extracted factor (referred to as Awareness of security risks) are graphically depicted in Figure 5.

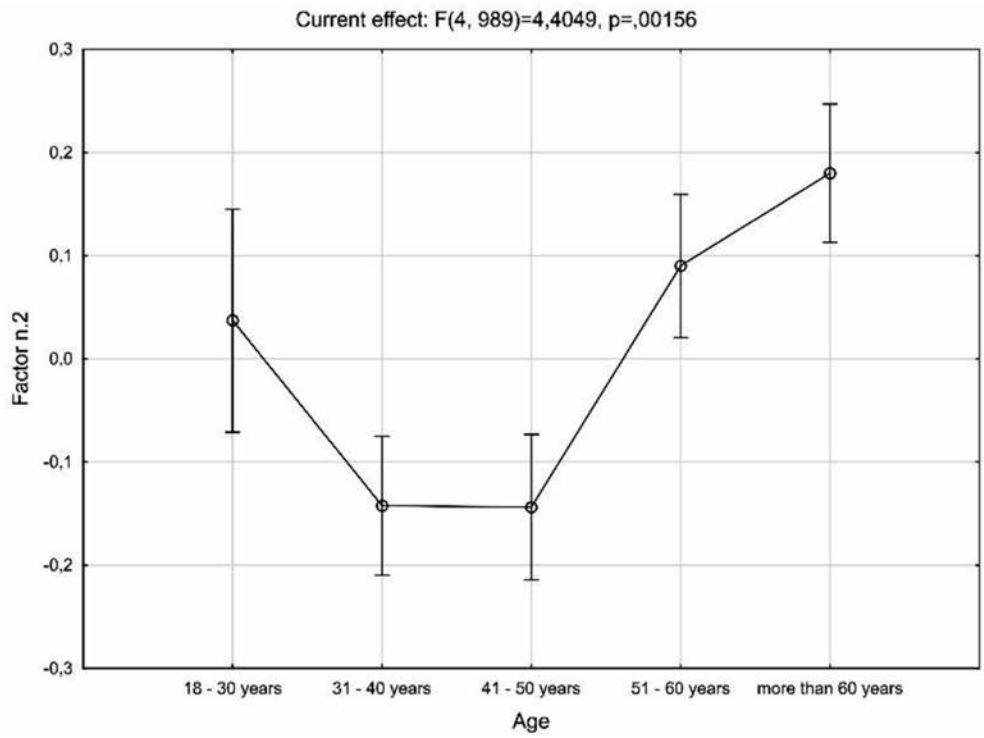

Figure 5. The dependence of average value of factor score for Factor 2 on age of respondents

Source: Own study

The second factor significantly influencing the value of achieved factor score for the second extracted factor is that relating to education of respondents. This implies from Table 5 based on the achieved levels of significance (p=0.000000). The average value of achieved factor score for respondents with primary education is -0.197575±0.127074, which indicates a negative perception of the problem of awareness of security risks and its importance for the latter category of respondents. Equally negative values of factor score are also those achieved for the group of respondents with secondary education, in whom, however, the average value is only -0.039588±0.096050. The values of factor score for respondents with university education are positive and achieve the average of 0.272641±0.086965. It is only the category of respondents with university education,

in whom the awareness of security risks becomes important. The average values of factor score for individual education categories for the second extracted factor (referred to as Awareness of security risks) are graphically depicted in Figure 6.

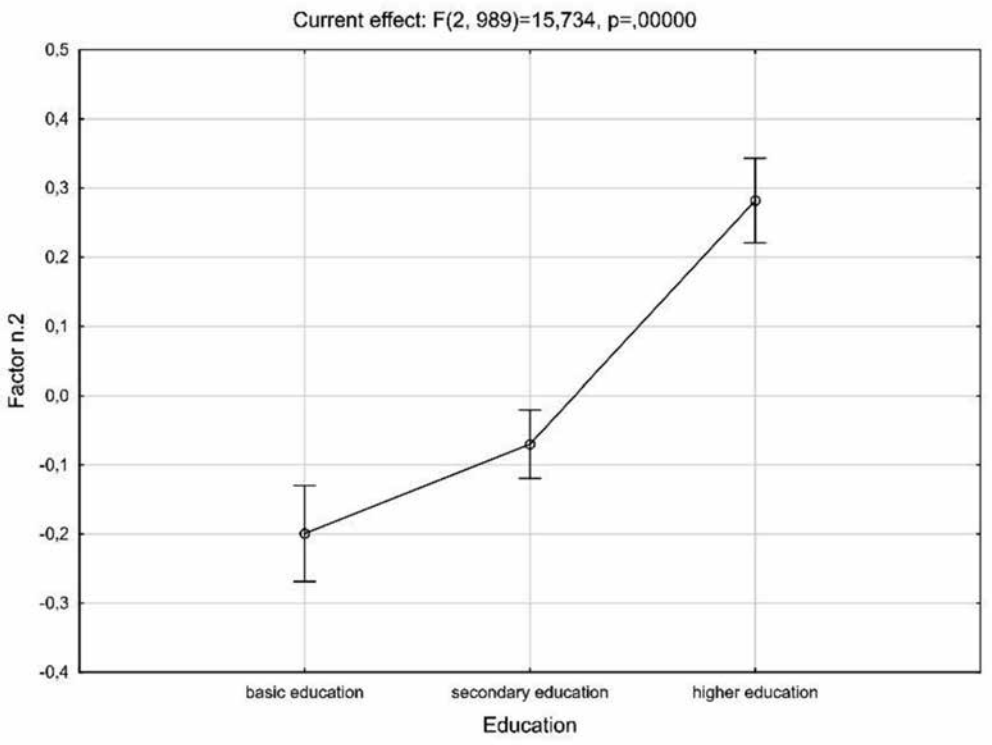

Figure 6. The dependence of average value of factor score for Factor 2 on education of respondents

Source: Own study

The Table 5 further shows that based on the level of significance (p=0.005595), the average value of achieved factor score for the second extracted factor referred to as Awareness of security risks is significantly influenced also by the interaction of age and education of respondents. This is illustrated in Figure 7.

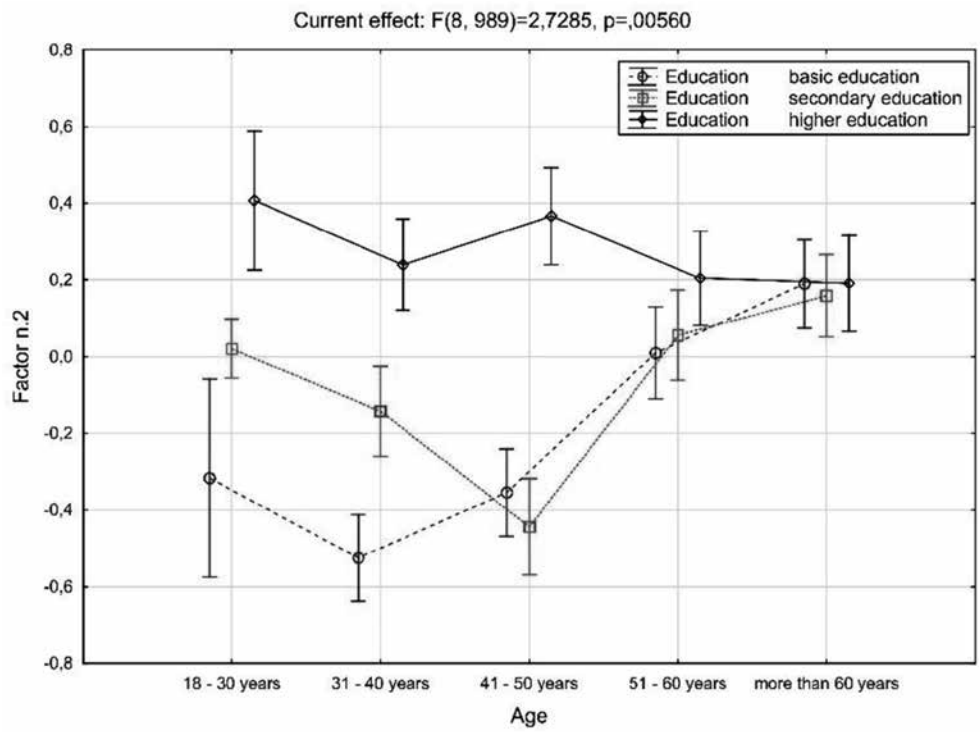

Figure 7. The dependence of average value of factor score for Factor 2 on interaction of age and education of respondents

Source: Own study

The Figure 7 shows that in respondents with primary and secondary education, the awareness of security risks associated with payment cards occurs in the negative part of bipolar scale, which indicates that they tend to underestimate the possible risks. Nevertheless, these two groups yield a change in the perception of security risks, namely in the category over 51 years of age. This change can be explained by information campaigns on security risks targeted at older age categories. The basic statistical characteristics of values of factor score for the interaction of age and education are given in Table 6.

Table 6. Statistical characteristics of the achieved factor score for Factor 2 and interaction of age and education of respondents

Effect	Level of Factor	Level of Factor	N	Factor n.2 Mean	Factor n.2 Std.Dev.	Factor n.2 Std.Err	Factor n.2 -95,00%	Factor n.2 +95,00%
Age*Education	18 - 30 years	basic education	17	-0,312875	0,884238	0,214459	-0,76751	0,141758
Age*Education	18 - 30 years	secondary education	160	0,017704	1,044045	0,082539	-0,14531	0,180718
Age*Education	18 - 30 years	higher education	29	0,411161	0,865402	0,160701	0,08198	0,740343
Age*Education	31 - 40 years	basic education	75	-0,572878	1,327718	0,153312	-0,87836	-0,267398
Age*Education	31 - 40 years	secondary education	68	-0,141994	1,147753	0,139186	-0,41981	0,135821
Age*Education	31 - 40 years	higher education	69	0,235276	0,836259	0,100674	0,03438	0,436168
Age*Education	41 - 50 years	basic education	72	-0,352274	1,133427	0,133576	-0,61862	-0,085932
Age*Education	41 - 50 years	secondary education	60	-0,453341	1,073022	0,138527	-0,73053	-0,176150
Age*Education	41 - 50 years	higher education	60	0,392295	0,596288	0,076980	0,23826	0,546333
Age*Education	51 - 60 years	basic education	65	0,011388	1,029397	0,127681	-0,24368	0,266460
Age*Education	51 - 60 years	secondary education	68	0,051129	0,916058	0,111088	-0,17060	0,272862
Age*Education	51 - 60 years	higher education	63	0,212590	0,711864	0,089686	0,03331	0,391871
Age*Education	more than 60 years	basic education	71	0,192051	0,809691	0,096093	0,00040	0,383702
Age*Education	more than 60 years	secondary education	82	0,161062	0,831747	0,091851	-0,02169	0,343817
Age*Education	more than 60 years	higher education	60	0,192059	0,719194	0,092848	0,00627	0,377847

Source: Own study

The initial results presented in Table 5 do not sufficiently answer the basic question as to which age and education groups of respondents differ from each other in relation to the value of achieved factor score. A more profound understanding of the differences between individual significant factors influencing the change in average value of factor score for the second extracted factor can be aided with the use of Scheffe's test.

Table 7. The result of Scheffe's test per age category and value of factor score for Factor 2

Cell No.	Scheffe test; variable Factor n.2 Probabilities for Post Hoc Tests Error: Between MS = ,93904, df = 989,00					
	Age	**{1} ,04581**	**{2} -,1716**	**{3} -,1512**	**{4} ,08985**	**{5} ,18012**
1	18 - 30 years		0,262373	0,392326	0,994972	0,733607
2	31 - 40 years	0,262373		0,999751	0,116414	0,007567
3	41 - 50 years	0,392326	0,999751		0,200032	0,019352
4	51 - 60 years	0,994972	0,116414	0,200032		0,926509
5	more than 60 years	0,733607	0,007567	0,019352	0,926509	

Source: Own study

Table 7 shows that for the level of significance of α=5 %, there exists a significant difference in the average value of the achieved factor score between age category older than 60 years and that in range of 31-40 years of age, as well as between the former age category and that in range of 41-50 years of age. On the other hand, all other differences between individual categories can be attributed to chance while at the level of significance of α=5 %, it is possible to consider them equal. Right here, it is necessary to indicate that in relation to age and preceding analyses, especially the younger age categories are not aware of risks arising from the use of payment cards.

Table 8. The result of Scheffe's test per education category and value of factor score for Factor 2

Cell No.	Scheffe test; variable Factor n.2 Probabilities for Post Hoc Tests Error: Between MS = ,93904, df = 989,00			
	Education	**{1} -,1976**	**{2} -,0396**	**{3} ,27264**
1	Primary education		0,094359	0,000000
2	Secondary education	0,094359		0,000150
3	University education	0,000000	0,000150	

Source: Own study

The results of Scheffe's test (Tab. 8) indicate that for the level of significance of 5 %, there is a significant mutual difference between the average value of achieved factor score between respondents with university education and those with secondary and primary education. On the other hand, no significant difference in average value of achieved factor score at the level of significance of 5 % was demonstrated between the respondents with primary education and those with secondary education, while the really occurring differences cannot be attributed to chance.

Conclusions

After extracting the significant factor 2 which is composed of three components (Q4: Do you consider ATMs located at banks' premises safer for withdrawing your cash?; 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?), it becomes clear that the attitude of respondents to the problem of awareness of security risks arising with using payment cards is influenced foremostly by their age, education and mutual interaction of the two latter attributes. The analysis of data revealed that for withdrawing cash, 75.24 % of respondents at age of 18-30 years prefer ATMs located at the premises of banks while as many as 16.02 % of respondents of the same age category do not trust the latter ATMs. A similar percentage of respondents at the

age of 31-40 years (75.47 %) equally prefer withdrawing cash from ATMs located at banks while 16.89 % of respondents of the latter age category are not concerned. The category of respondents at age of 41-50 years trust ATMs located at banks in 73.96 % which represents a decrease compared to younger categories of respondents. However, as many as 86.73 % of respondents in category of 51-60 years of age prefer ATMs located at banks while the latter ATMs are preferred by 86.85 % of respondents over 60 years of age. When we inspect the question of trust associated with cash withdrawal from the aspect of education, then ATMs located in the premises of banks are preferred by 74.67 % of respondents with primary education, 79.22 % of respondents with secondary education and as many as 85.77 % of those with university education. The second component of the research tool participating in creating the second extracted factor, namely the component Q13 (Do you think that the payment system carries elements of high security risks?) represents the key component of the latter factor. The analysis reveals that as many as 93.20 % of respondents at age of 18-31 years is aware of security risks arising from using payment systems while only 0.49 % is not aware of these risks. The category at age of 31-40 years yields surprising results, namely that as many as 80.19 % of respondents are aware of the risks, however, this is a smaller proportion from all analyzed age categories while as many as 8.49 % are not aware of these risks, which on the other hand is the highest value from all age categories. Respondents from categories over 41 years of age are aware of security risks at the level of ca 86 %, which represents a positive finding of this analysis. From the aspect of education and awareness of security risks arising from the use of payment systems, we come to a conclusion that 81.67 % of respondents with primary education are aware of these risks, while 7.00 % of the latter category are not. The analysis further reveals that 83.56 % of respondents are aware of security risks arising from the use of payment systems, while in the category of those with university education, the latter percentage is higher, namely 95.73 %. These results are the base for concluding that people with higher education are better informed and thus more aware of the risks arising from the use of the payment system, even though in general, regardless of education, the proportion of aware respondents is relatively high, namely 86.99 %. In conclusion it is necessary to state that the dispersion analysis as a whole is statistically significant at the level of α=5 % (p=0.0000). Naturally, a more profound analysis of other extracted factors would be necessary for achieving a comprehensive understanding and depiction of users' behaviors and risks in the field of security of payment instruments. Unfortunately, the scope of present analysis is not that extensive. However, the authors intend to analyze further factors with the use of multidimensional statistical methods.

References

Abbey, D.C. (2018) Prospective Payment Systems, Productivity Press Inc. ©2018, ISBN:113844037X 9781138440371

Bányász, P. (2018) Media and Terrorism, Academic and Applied Research in Military and Public Management Science Vol. 17, No. 3 (2018) 47–62.47, Social ISSN 2498-5392

Batkovskiy, A.M., Leonov, A.V., Pronin, A.Yu., Semenova, E.G., Fomina, A.V., Balashov, V.M. (2019) Sustainable development of Industry 4.0: the case of high-tech products system design, Entrepreneurship and Sustainability Issues 6(4): 1823-1838. http://doi.org/10.9770/jesi.2019.6.4(20)

Bayuk, J.L., Healey, J., Rohmeyer, P., Sachs, M., Schmidt, J., Weiss, J. (2012) Cyber Security Policy Guidebook, Wiley Publishing ©2012, ISBN: 1118027809 9781118027806

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)

Federal Reserve Bank of Chicago. "Second Quarter 2006, Volume XXX, Issue 2," *Economic Perspectives (Federal Reserve Bank of Chicago)* (Second Quarter 2006). https://fraser.stlouisfed.org/title/5288/item/579026

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

Horecký, J. (2018). Operation and action of a trade union (in terms of Czech Republic labour law). Central European Journal of Labour Law and Personnel Management, 1(1): 17 – 27. http://doi.org/10.33382/cejllpm.2018.01.02

Chakravorti, S. (2016) New Payment Technologies: Back to Basicsin Digital Transformation of Payment Media conference organized by Funcas, May 26, 2016 in Madrid, Spain. http://doi.org/10.2139/ssrn.2781264

Christiansen, B., Piekarz, A. (2019) Global Cyber Security Labor Shortage and International Business Risk, IGI Global publishing, USA, ISSN 2327-3429

Davidavičienė, V., Raudeliūnienė, J., Tvaronavičienė, M., Kaušinis, J. (2019) The importance of security aspects in consumer preferences in electronic environment, Journal of Security and Sustainability Issues, 8(3): 399-411. http://doi.org/10.9770/jssi.2019.8.3(9)

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.; Kelemen, P. 2019a. Security position and detection of unusual business operations from science and research perspective, Entrepreneurship and Sustainability Issues*,* 6(3):1270-1279. http://doi.org/10.9770/jesi.2019.6.3(15)

Korauš, A., Dobrovič, J., Polák, J., Backa, S. 2019b. 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)

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., Agafonov K., Paukštė L., Damkus, M., Plėta T. 2017. Peculiarities of cyber security management in the process of internet voting implementation, *Entrepreneurship and Sustainability Issues* 5(2): 368-402. http://doi.org/10.9770/jesi.2017.5.2(15)

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.

Marty, R., (2013) Cyber security: how visual analytics unlock insight, KDD '13 Proceedings of the 19th ACM SIGKDD international conference on Knowledge discovery and data mining, Pages 1139-1139, Chicago, Illinois, USA — August 11 - 14, 2013
ACM New York, NY, USA ©2013, ISBN: 978-1-4503-2174-7, http://doi.org/10.1145/2487575.2491132

Mura, L., Buleca, J., Hajduová, Z., Andrejkovič, M. (2015). Quantitative Financial Analysis of Small and Medium Food Enterprises in a Developing Country. Transformation in Business & Economics, 141(34): 212 – 224. ISSN 1648-4460

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. https://doi.org/10.5593/sgem2017/51/S20.079

Okanazu, O. O. (2018). Financial management decision practices for ensuring business solvency by small and medium scale enterprises. Acta Oeconomica Universitatis Selye 7(2): 109 – 121. ISSN 1338-6581

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

PYMNTS.COM (2016), Faster Payments Tracker, powered by NACHA, May https://www.pymnts.com/

Radu, C. (2002) Implementing Electronic Card Payment Systems, Artech House, Inc. Norwood, MA, USA ©2002, ISBN:1580533051

Ras, J. (2016) Cyber Security, Lulu.com ©2016, ISBN:1365288234 9781365288234

Schwab, K. (2018) Global Competitiveness Report 2018, World Economic Forum91-93 route de la CapiteCH-1223 Cologny/ GenevaSwitzerland. ISBN-13: 978-92-95044-76-0

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)

Thapliyal, K., Pathak, A., Banerjee, S. (2017) Quantum cryptography over non-Markovian channels, Journal Quantum Information Processing, Volume 16 Issue 5, May 2017, Kluwer Academic Publishers Hingham, MA, USA,
https://doi.org/10.1007/s11128-017-1567-1

Tvaronavičienė M. (2018) Towards internationally tuned approach towards critical infrastructure protection, Journal of Security and Sustainability Issues 8(2): 143-150. https://doi.org/10.9770/jssi.2018.8.2(2)

Veselovská, S.; Korauš, A.; & Polák, J. (2018). Money Laundering and Legalization of Proceeds of Criminal Activity, *Second International Scientific Conference on Economics and Management - EMAN 2018*, March 22, Ljubljana, Slovenia, Printed by: All in One Print Center, Belgrade, 2018, ISBN 978-86-80194-11-0 https://doi.org/10.31410/EMAN.2018

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

JUDr. Stanislav BACKA, Ph.D. Candidate at the Faculty of Management at the University of Prešov in Prešov, Slovak Republic
ORCID ID: https://orcid.org/0000-0002-0411-4158