Computing, Information Systems & Development Informatics Journal
Vol. 9 No. 4, December, 2018 - www.cisdijournal.org

Computing, Information Systems Development Informatics & Allied Research Journal

Vol. 9. No. 4. December, 2018

An International Publication of
The African Society for Information & Communication Technology
In Collaboration with
The Institute of Development Informatics & Policy, Ghana

December, 2018

ISSN: 2167-1710

cisdi Journal
Computing, Information Systems & Development Informatics Journal
Vol. 9 No. 4, December, 2018 - www.cisdijournal.org

CONTENTS

Computing, Information Systems & Development Informatics Journal
Vol. 9 No. 4, December, 2018 - www.cisdijournal.org

Editorial Board

Computing, Information Systems & Development Informatics Journal
Vol. 9 No. 4, December, 2018 - www.cisdijournal.org

Preface to this Edition of the CISDI Journal

This volume of the CISDI Journal in 2017 provides a distinctive international perspective on theories, issues, frameworks and practice at the nexus of computing, information systems Developments Informatics, Business Management, Behavioural Sciences and policy. A new wave of multidisciplinary research efforts is required to provide pragmatic solution to most of the problems the world faces today. With Computing and Information Technology (IT) providing the needed momentum to drive growth and development in different spheres of human endeavours, there is a need to create platforms through which breakthrough research and research findings that cuts across different discipline can be reported. Such dissemination to a global audience will in turn support future discoveries, sharpen the understanding of theoretical underpinnings and improve practices. This is exactly what the CISDI Journal aims to achieve with timely publications of research, cases and findings from practices in the domain of Computing, Information Technology, Information System/Science, Business, Management, Behavioural Sciences, Social Sciences, Development Informatics and other allied domain.

We encourage you to read through this volume and consider submitting articles that reports cutting edge research in computing and short communications/reviews in development informatics research that appropriate design, localization, development, implementation and usage of information and communication technologies (ICTs) to achieve development goals. The CISDI Journal accept articles that promote policy research by employing established (and proposed) legal and social frameworks to support the achievement of development goals through ICTs - particularly the millennium development goals. We will also consider for acceptance, academically robust papers, empirical research, case studies, action research and theoretical discussions which advances learning within the Journal scope and target domains. Extended versions and papers with approved copyright release previously presented at conferences, workshops and seminars will also be accepted for publication.

We welcome feedbacks and rejoinders

Enjoy your reading

Thank you

Longe Olumide Babatope PhD
Professor, Distinguished Fulbright Alumni & Managing Editor
CISDI Journal
E-mail: submissions@cisdijournal.net

Computing, Information Systems & Development Informatics Journal
Vol. 9 No. 4, December, 2018 - www.cisdijournal.org

Security Risk Analysis and Management in GSM Operations Using MTN as a Case Study.

Ndatsu Z, Adebayo, O.S. & Ojeniyi, J.
Department of Cyber Security Science
The Federal University of Technology
Minna, Niger State, Nigeria
E-mail: zainab.pg6717@st.futminna.edu.ng, waleadebayo@futminna.edu.ng , ojeniyija@futminna.edu.ng

ABSTRACT

Risk analysis is a process that helps identify and manage potential problems that could undermine key business processes. Security risk analysis on GSM operations using MTN as a case study was carried out in this research. The objective is to ensure confidentiality, integrity and availability of GSM operations. Our motivation for takling risk analysis is that small business owners take risks every day putting too much at stake and their businesses in the long run could suffer. Qualitative method was used for this research where 70 Questionnaire was prepared and distributed to users of MTN using five components of the business processes measures and 50 were received, as duly completed by the users of the products in context. Chi square was used in the analysis to determine where there is association between mobile electricity, mobile app., SIM card, recharge card, customer name and security. The p - values of chi square of analysis is greater than 0.05 indicating independence in association between security, mobile electricity, mobile app, recharge card, SIM card and customer name. Findings revealed the sucesptibility to risks by business owners which then necessitate our reccomendations that MTN should put into consideration security of the components .

Keywords: Security analysis, risk analysis and management, MTN operations & GSM operations.

CISDI Journal Reference Format
Ndatsu Z, Adebayo, O.S. & Ojeniyi, J. (2018): Security Risk Analysis and Management in GSM Operations Using MTN as a Case Study. Computing, Information Systems & Development Informatics Journal. Vol. 9 No. 4. Pp 1-14. Available online at www.cisdijournal.net

1. INTRODUCTION

The telecommunications industry is currently Nigeria's second most important beneficiary of FDI after the extractive oil industry (Nigeria Bureau of Statistics, 2013). Another interesting statistic of the Nigerian telecoms industry is the origin of the foreign direct investment(FDI) in the industry (Osabutey & Okoro, 2015).The two types of risk analysis methods are Quantitative risk analysis methods which use mathematical and statistical tools to represent risk and qualitative risk analysis methods where risk is analyzed with the help of adjectives instead of using mathematics. Risk analysis methods which use intensive quantitative measures are not suitable for today's information security risk analysis (Karabacak & Sogukpinar, 2005). It is said that poor risk analysis brings more risk to a business. Also, risk analysis cannot be considered as independent from risk response stage and the contract strategy. The assumptions made in the risk analysis stage determine the overall success of the risk management process (Dikmen, Birgonul, & Arikan, n.d, 2004). The loss of confidentiality, integrity, availability, accountability, authenticity and reliability of information and services can have harmful impacts on M commerce.(Seify & Bijani, 2009)

This research work has the following sections, section one is the introduction, two is the related works, three is the method, four is the result and discussion, five is the conclusion and finally six is the recommendation.

2. RELATED WORKS

Seify & Bijani (2009) based on the risk analysis done in the GSM network of Iran a methodology for cellular mobile network risk management is established. Fluorescent proteins with light wavelengths within the optical window are one of the improvements in in vivo imaging techniques (Tran et al., 2014). This means that it is important and strategic to consider how much impact political risk influenced the FDI flows in the Nigerian telecommunications industry (Osabutey & Okoro, 2015). With the introduction of GSM devices, use of ebook readers such as iPad and Kindle and the success of social networking giants such as Facebook, the demand for mobile data traffic has also grown significantly in recent years. Hence, mobile users find meeting these new demands in wireless mobile networks inevitable, while they have to keep their costs minimum (Hasan, Boostanimehr, & Bhargava, 2011).

This paper describe the risks to electronic security via identity theft, hacking, etc. that wireless technologies may present in the context of delivery of financial services. Although the extent of security measures to be taken is not independent of the size of the transactions contemplated, the paper points out a variety of ways that interactions between technologies create points of vulnerability for security of financial transactions when wireless technology is used (Kellermann, n.d. 2002). The paper used a novel method and ISRAM, is proposed for information security risk analysis.

The proposed method was based on a quantitative approach that uses survey results to analyze information security risks (Karabacak & Sogukpinar, 2005). Authors of this paper try to develop a Risk Management support tool which is capable of identification of relationship between risk sources, consequences, responses and project success criteria, and integrating all tasks of risk management.(Dikmen et al., n.d.).

This paper discuss tools for seismic risk and loss assessment but the tool are underdevelopment(Molina, Lang, & Lindholm, 2010)

3. METHOD

In a bid to get the views and opinions of users of MTN product, 70 questionnaires were printed for this fact-finding on security risk pose on the products. 49 questionnaires were received, as duly completed by the users of products, at the conclusion of the survey. The questionnaires were designed using a 5-scale response pattern comprising which are Very low =1, Low = 2, Medium =3, High = 4, Very high = 5 and IBM SPSS statistics 23 was used to analyzed the result of table 1 below. The survey was carried out at Federal Polytechnic, Bida , Federal University of Technology Minna and out the schools campus in Nigeria. Thus stated below is a summary of the survey and analysis:

Table1. The five (5) component used with the frequency generated from the questionnaires

	Very low	low	Medium	High	Very high
Mobile electricity					
Cost of relation	6	3	6	1	1
Cost of modification	3	4	4	4	2
Loss of access	5	4	3	3	2
Mobile app.					
Cost of relation	5	4	2	4	3
Cost of modification	4	3	4	5	2
Loss of access	4	5	7	1	1
SIM card number					
Cost of relation	2	5	4	3	2
Cost of modification	3	3	2	2	6
Loss of access	3	3	7	2	2
Recharge card					
Cost of relation	5	3	1	5	7
Cost of modification	2	3	4	6	3
Loss of access	2	2	2	4	7
Customer name					
Cost of relation	2	5	5	4	1
Cost of modification	4	2	7	1	4
Los of access	1	4	5	3	3

4. RESULT AND DISCUSSION

The following are result analysis generated from IBM SPSS statistics 23 using table 1 above

Table 2: Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
mobile_electricity * security	51	100.0%	0	0.0%	51	100.0%

From table 2 there are 51 participants in the survey and no missing value so therefore our judgment on the association between mobile electricity and security is going to be based on the fifty-one (51) participant.

Table 2.1: mobile_electricity * security Crosstabulation

			security			
			lost_access	modification	revelation	Total
mobile_electricity	high	Count	3	4	1	8
		Expected Count	2.7	2.7	2.7	8.0
		% within security	17.6%	23.5%	5.9%	15.7%
	low	Count	4	4	3	11
		Expected Count	3.7	3.7	3.7	11.0
		% within security	23.5%	23.5%	17.6%	21.6%
	medium	Count	3	4	6	13
		Expected Count	4.3	4.3	4.3	13.0
		% within security	17.6%	23.5%	35.3%	25.5%
	Very high	Count	2	2	1	5
		Expected Count	1.7	1.7	1.7	5.0
		% within security	11.8%	11.8%	5.9%	9.8%
	Very low	Count	5	3	6	14
		Expected Count	4.7	4.7	4.7	14.0
		% within security	29.4%	17.6%	35.3%	27.5%
Total		Count	17	17	17	51
		Expected Count	17.0	17.0	17.0	51.0
		% within security	100.0%	100.0%	100.0%	100.0%

From table 2.1 we can see that dependent variable is mobile electricity the influencing variable is the security. In the first column 3 participant choose that security impact on loss of access to mobile electricity is high, 4 participants chooses that security impact is low, 3 chooses is medium, 2 chooses very high and 5 choose that it is very low. Second column is the security impact in modification of mobile electricity 4 participant choose it high, 4 participant choose that it is low, 4 choose medium,2 choose very high and 3 choose very low. Third column is the security impact in cost of revelation of mobile electricity 1 participant choose it high, 3 participant choose that it is low, 6 choose medium,1 choose very high and 6 choose very low.

Table 2.2: Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	4.409[a]	8	.818
Likelihood Ratio	4.727	8	.786
N of Valid Cases	51		

a. 15 cells (100.0%) have expected count less than 5. The minimum expected count is 1.67.

From table 2.2 above chi square value 4.409 and degree of freedom is 8, p- value is 0.818 indicating that null hypothesis should be accepted that is the association between security and mobile electricity is independent.

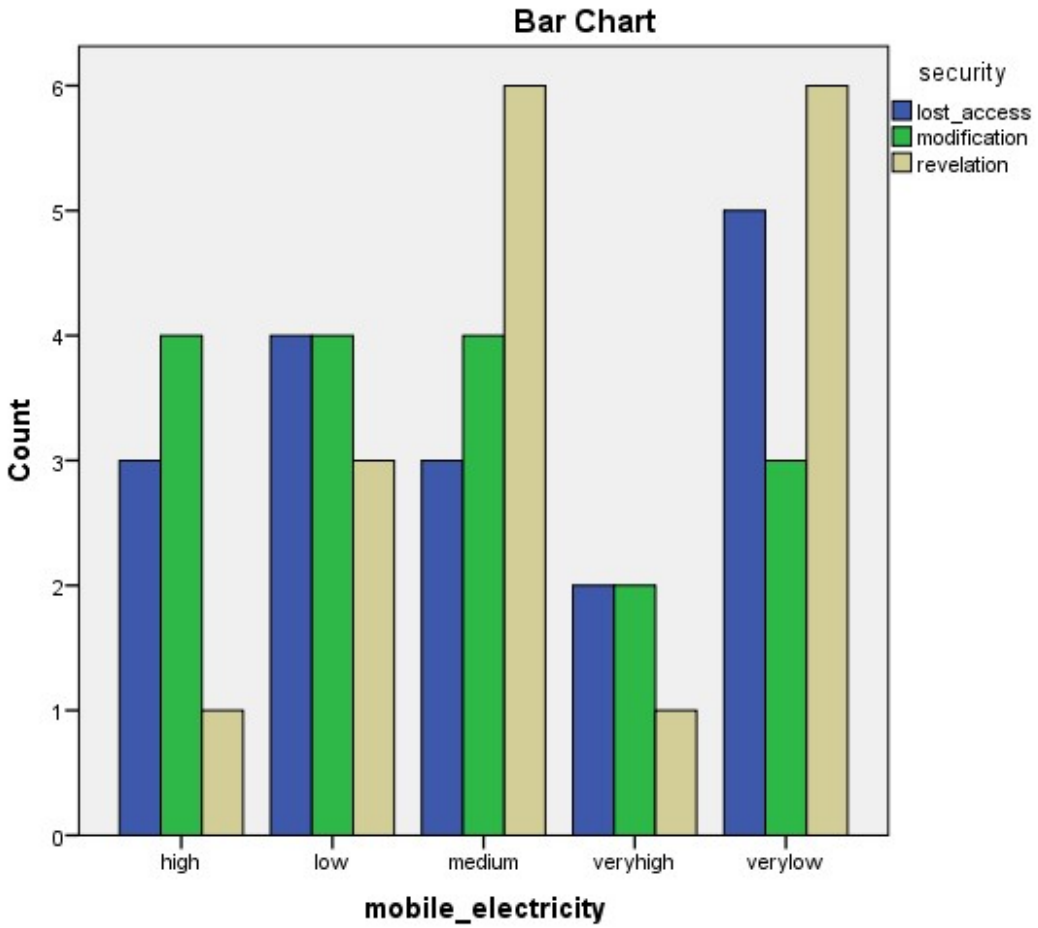

Figure 1: Bar chart representation of responses for mobile electricity

Figure 1 above show bar chart represent of responses for mobile electricity which shows that cost of revelation is medium, cost of modification is between medium and high and cost of lost of access is very low.

Table 3: Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
mobile_app * security	54	100.0%	0	0.0%	54	100.0%

From table 3 there are 54 participants in the survey and no missing value so therefore our judgment on the association between mobile app and security is going to be based on the fifty-four (54) participant.

Table 3.1 mobile_app * security Cross tabulation

			security			Total
			lost_access	modification	revelation	
mobile_app	high	Count	1	5	4	10
		Expected Count	3.3	3.3	3.3	10.0
		% within security	5.6%	27.8%	22.2%	18.5%
	low	Count	5	3	4	12
		Expected Count	4.0	4.0	4.0	12.0
		% within security	27.8%	16.7%	22.2%	22.2%
	medium	Count	7	4	2	13
		Expected Count	4.3	4.3	4.3	13.0
		% within security	38.9%	22.2%	11.1%	24.1%
	veryhigh	Count	1	2	3	6
		Expected Count	2.0	2.0	2.0	6.0
		% within security	5.6%	11.1%	16.7%	11.1%
	verylow	Count	4	4	5	13
		Expected Count	4.3	4.3	4.3	13.0
		% within security	22.2%	22.2%	27.8%	24.1%
Total		Count	18	18	18	54
		Expected Count	18.0	18.0	18.0	54.0
		% within security	100.0%	100.0%	100.0%	100.0%

From table 3.1 we can see that dependent variable is mobile app the influencing variable is the security. In the first column 1 participant choose that security impact on loss of access to mobile app. is high, 5participants chooses that security impact is low, 7 chooses is medium, 1 chooses very high and 4 choose that it is very low. Second column is the security impact in modification of mobile electricity 5 participant choose it high, 3 participant choose that it is low, 4 choose medium,2 choose very high and 4 choose very low. Third column is the security impact in cost of revelation of mobile electricity 4 participant choose it high, 4 participant choose that it is low, 2 choose medium,3 choose very high and 5 choose very low.

Table 3.2 Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	7.177[a]	8	.518
Likelihood Ratio	7.788	8	.454
N of Valid Cases	54		

a. 15 cells (100.0%) have expected count less than 5. The minimum expected count is 2.00.

From table 3.2 above chi square value 7.177 and degree of freedom is 8, p- value is 0.518 indicating that null hypothesis should be accepted that is the association between security and mobile app. is independent.

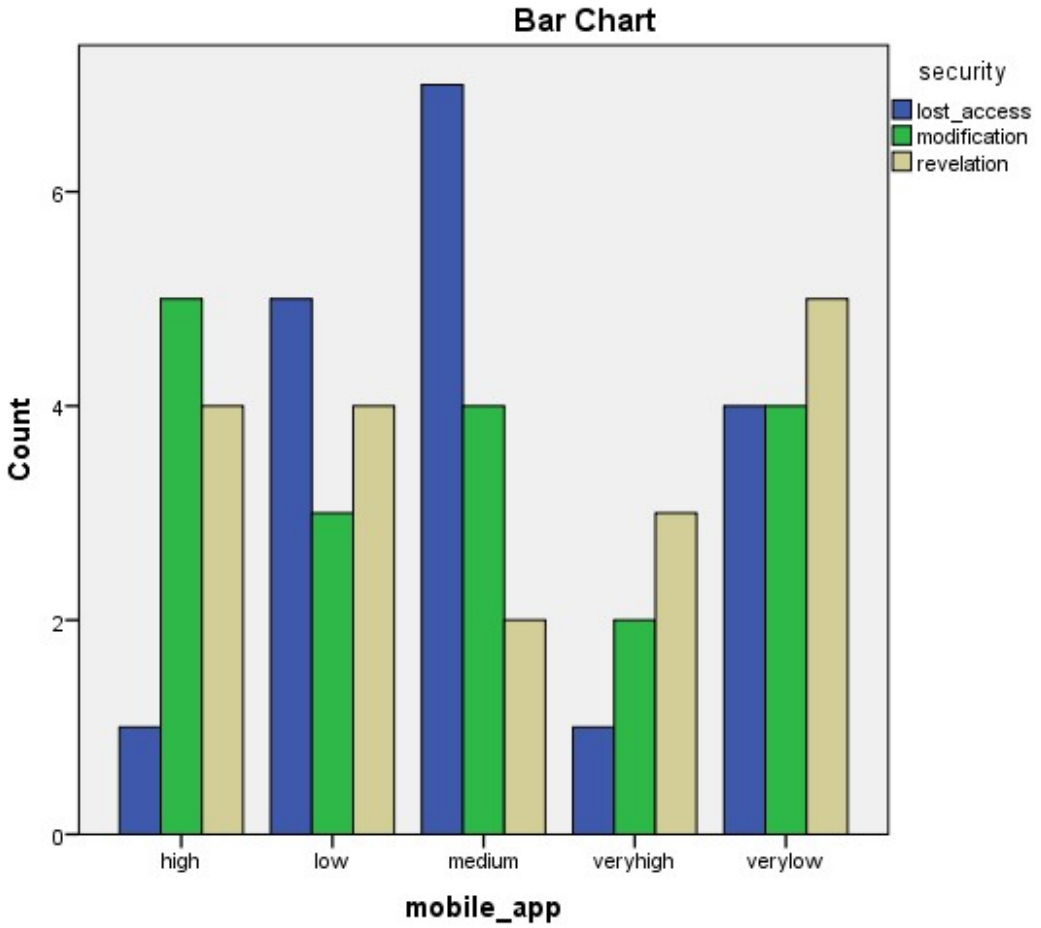

Figure 2: Bar chart representation of responses for mobile app

Figure 2 above show bar chart represent of responses for mobile app which shows that cost of revelation is very low, cost of modification is high and cost of lost of access is medium.

Table 4: Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
sim_card * security	49	100.0%	0	0.0%	49	100.0%

From table 4 there are 49 participants in the survey and no missing value so therefore our judgment on the association between sim card and security is going to be based on the forty nine (49) participants.

Table 4. 1: sim_card * security Crosstabulation

			security			
			lost_access	modification	revelation	Total
sim_card	high	Count	2	2	3	7
		Expected Count	2.4	2.3	2.3	7.0
		% within security	11.8%	12.5%	18.8%	14.3%
	low	Count	3	3	5	11
		Expected Count	3.8	3.6	3.6	11.0
		% within security	17.6%	18.8%	31.3%	22.4%
	medium	Count	7	2	4	13
		Expected Count	4.5	4.2	4.2	13.0
		% within security	41.2%	12.5%	25.0%	26.5%
	veryhigh	Count	2	6	2	10
		Expected Count	3.5	3.3	3.3	10.0
		% within security	11.8%	37.5%	12.5%	20.4%
	verylow	Count	3	3	2	8
		Expected Count	2.8	2.6	2.6	8.0
		% within security	17.6%	18.8%	12.5%	16.3%
Total		Count	17	16	16	49
		Expected Count	17.0	16.0	16.0	49.0
		% within security	100.0%	100.0%	100.0%	100.0%

From table 4.1 we can see that dependent variable is SIM card the influencing variable is the security. In the first column 2 participant choose that security impact on loss of access to SIM card is high, 3 participants chooses that security impact is low, 7 chooses is medium, 2 chooses very high and 3 choose that it is very low. Second column is the security impact in modification of mobile electricity 2 participant choose it high, 3 participant choose that it is low, 2 choose medium,6 choose very high and 3 choose very low. Third column is the security impact in cost of revelation of mobile electricity 3 participant choose it high, 5 participant choose that it is low, 4 choose medium,2 choose very high and 2 choose very low.

Table 4.2: Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	7.357[a]	8	.499
Likelihood Ratio	7.138	8	.522
N of Valid Cases	49		

a. 15 cells (100.0%) have expected count less than 5. The minimum expected count is 2.29.

From table 4.2 above chi square value 7.357 and degree of freedom is 8 the p - value is 0.499 indicating that null hypothesis should be accepted that is the association between security and sim cardis independent.

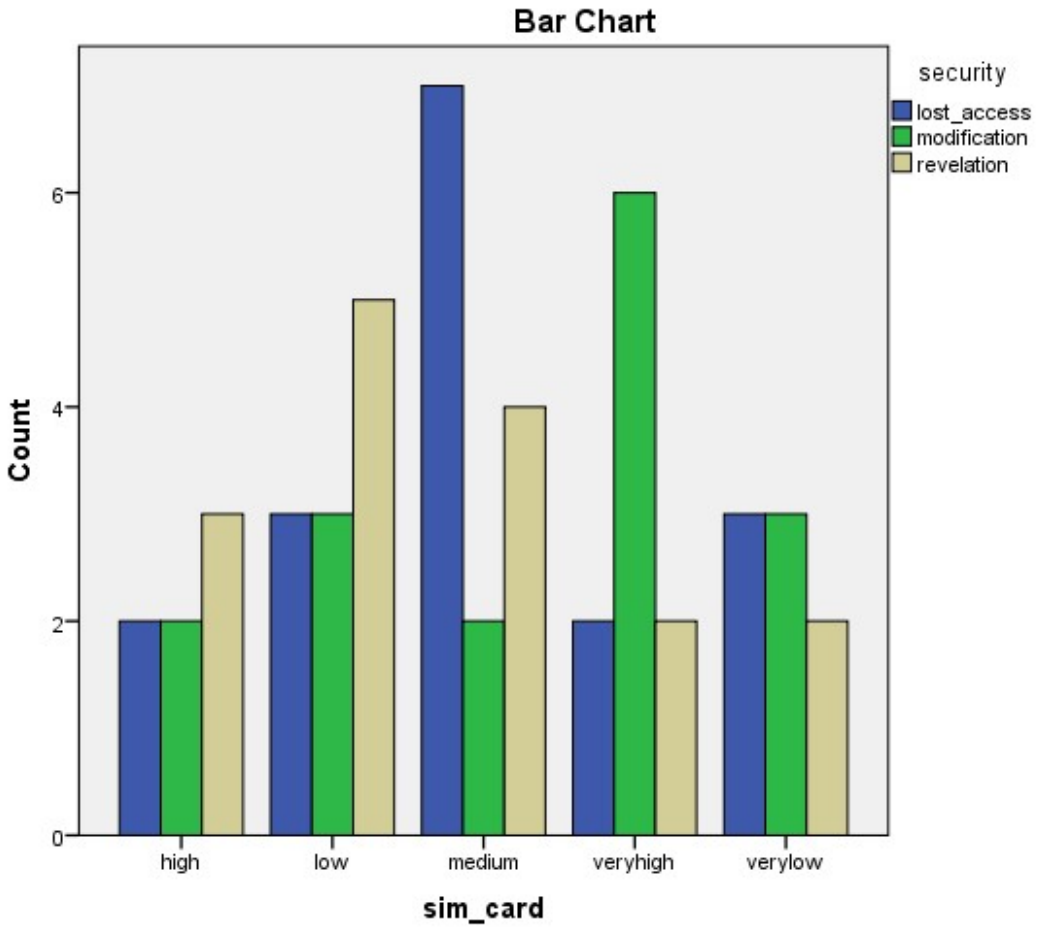

Figure 3: Graphical representation of responses for SIM card

Figure 3 above show graphical represent of responses for sim card which shows that cost of revelation is low, cost of modification is very high and cost of lost of access is medium.

Table 5: Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
recharge_card * security	56	100.0%	0	0.0%	56	100.0%

From table 5 there are 56 participants in the survey and no missing value so therefore our judgment on the association between recharge card and security is going to be based on the fifty-six (56) participants.

Table 5.1: recharge card * security Cross tabulation

			security			
			lost_access	modification	revelation	Total
recharge_card	high	Count	4	6	5	15
		Expected Count	4.6	4.8	5.6	15.0
		% within security	23.5%	33.3%	23.8%	26.8%
	low	Count	2	3	3	8
		Expected Count	2.4	2.6	3.0	8.0
		% within security	11.8%	16.7%	14.3%	14.3%
	medium	Count	2	4	1	7
		Expected Count	2.1	2.3	2.6	7.0
		% within security	11.8%	22.2%	4.8%	12.5%
	veryhigh	Count	7	3	7	17
		Expected Count	5.2	5.5	6.4	17.0
		% within security	41.2%	16.7%	33.3%	30.4%
	verylow	Count	2	2	5	9
		Expected Count	2.7	2.9	3.4	9.0
		% within security	11.8%	11.1%	23.8%	16.1%
Total		Count	17	18	21	56
		Expected Count	17.0	18.0	21.0	56.0
		% within security	100.0%	100.0%	100.0%	100.0%

From table 5.1 we can see that dependent variable is recharge card the influencing variable is the security. In the first column 4 participant choose that security impact on loss of access to recharge card is high, 2 participants chooses that security impact is low, 2 chooses is medium, 7 chooses very high and 2 choose that it is very low. Second column is the security impact in modification of mobile electricity 6 participant choose it high, 3 participant choose that it is low, 4 choose medium,3 choose very high and 2 choose very low. Third column is the security impact in cost of revelation of mobile electricity 5 participant choose it high, 3 participant choose that it is low, 1 choose medium,7 choose very high and 5 choose very low.

Table 5.2: Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	6.029[a]	8	.644
Likelihood Ratio	6.174	8	.628
N of Valid Cases	56		

a. 11 cells (73.3%) have expected count less than 5. The minimum expected count is 2.13.

From table 5.2 above chi square value 6.029 and degree of freedom is 8, p- value is 0.644 indicating that null hypothesis should be accepted that is the association between security and recharge card is independent.

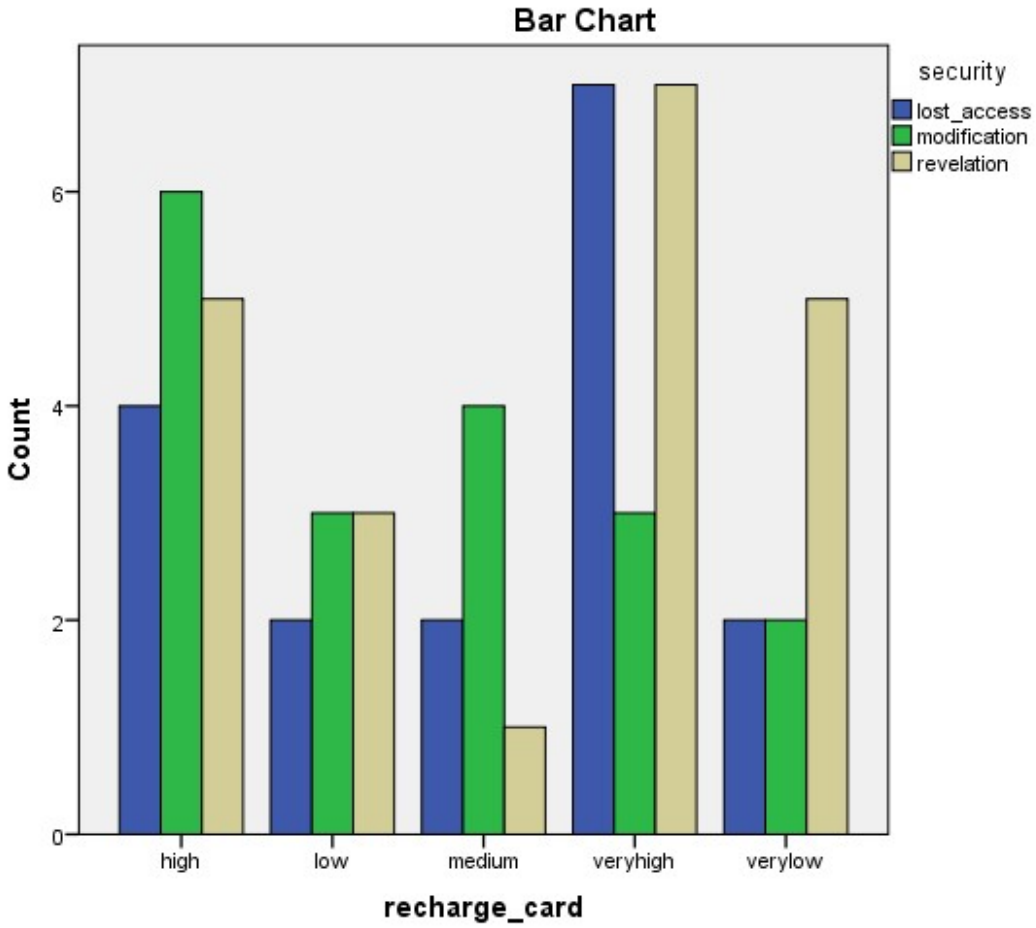

Figure 4: Bar chart representation of responses for recharge card

Figure 4 above show bar chart represent of responses for recharge card which shows that cost of revelation is very high, cost of modification is very high while cost of lost of access is high.

Table 6. Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
customer_name * security	51	100.0%	0	0.0%	51	100.0%

From table 6 there are 51 participants in the survey and no missing value so therefore our judgment on the association between customer name and security is going to be based on the fifty-one (51) participants.

Table 6. 1: customer_name * security Crosstabulation

			security			
			lost_access	modification	revelation	Total
customer_name	high	Count	3	1	4	8
		Expected Count	2.5	2.8	2.7	8.0
		% within security	18.8%	5.6%	23.5%	15.7%
	low	Count	4	2	5	11
		Expected Count	3.5	3.9	3.7	11.0
		% within security	25.0%	11.1%	29.4%	21.6%
	medium	Count	5	7	5	17
		Expected Count	5.3	6.0	5.7	17.0
		% within security	31.3%	38.9%	29.4%	33.3%
	very high	Count	3	4	1	8
		Expected Count	2.5	2.8	2.7	8.0
		% within security	18.8%	22.2%	5.9%	15.7%
	verylow	Count	1	4	2	7
		Expected Count	2.2	2.5	2.3	7.0
		% within security	6.3%	22.2%	11.8%	13.7%
Total		Count	16	18	17	51
		Expected Count	16.0	18.0	17.0	51.0
		% within security	100.0%	100.0%	100.0%	100.0%

From table 6.1 we can see that dependent variable is customer name the influencing variable is the security. In the first column 3 participant choose that security impact on loss of access to customer name is high, 4 participants chooses that security impact is low, 5 chooses is medium, 3 chooses very high and 1 choose that it is very low. Second column is the security impact in modification of mobile electricity 1 participant choose it high, 2 participant choose that it is low, 7 choose medium,4 choose very high and 4 choose very low.

Third column is the security impact in cost of revelation of mobile electricity 4 participant choose it high, 5 participant choose that it is low, 5 choose medium,1 choose very high and 2 choose very low.

Table 6.2: Chi-Square Tests

	Value	df	Asymptotic Significance (2-sided)
Pearson Chi-Square	6.964[a]	8	.540
Likelihood Ratio	7.689	8	.464
N of Valid Cases	51		

a. 12 cells (80.0%) have expected count less than 5. The minimum expected count is 2.20.

From table 6.2 above chi square value 6.964 and degree of freedom is 8, p- value is 0.540 indicating that null hypothesis should be accepted that is the association between security and customer name is independent.

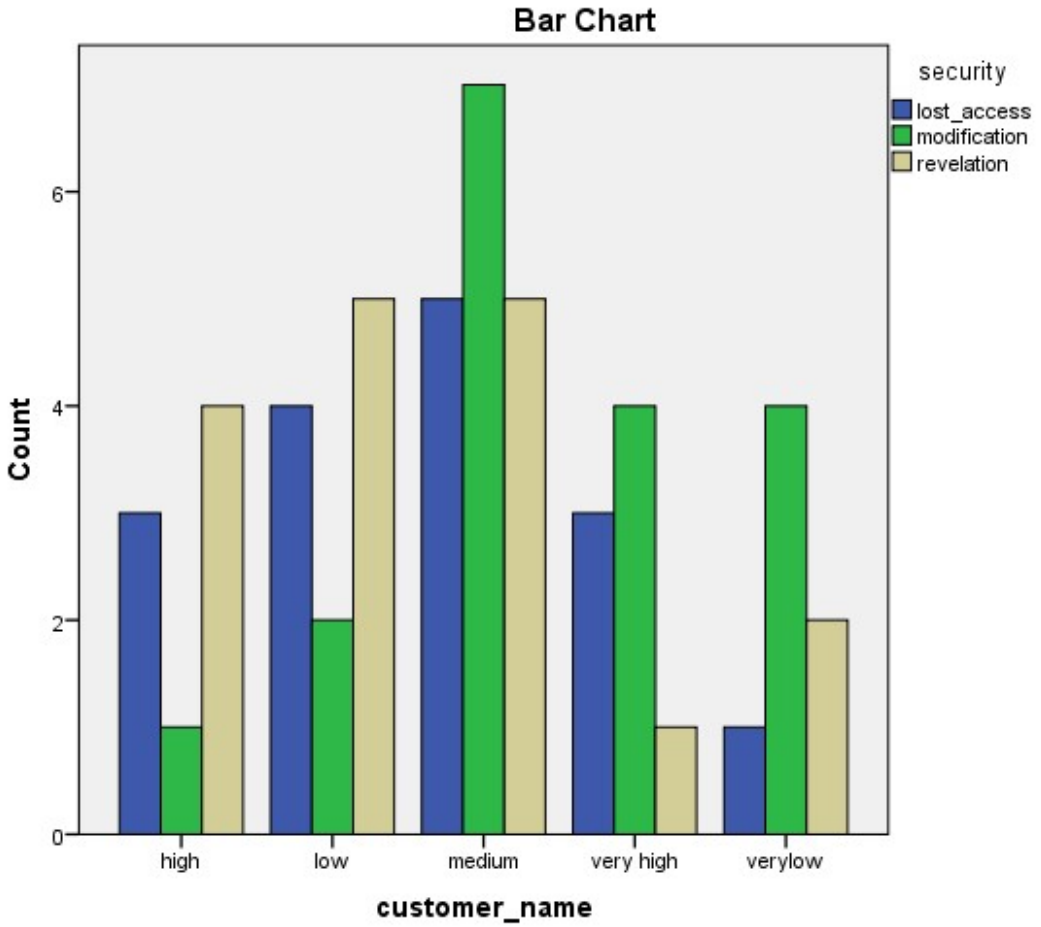

Figure 5: Bar chart representation of responses for customer name

Figure 5 above show bar chart represent of responses for customer name which shows that cost of revelation is low and medium, cost of modification is medium while cost of loss of access is medium.

5. CONCLUSION

There is evidence of independence between the association security, mobile electricity, mobile app, SIM card, and customer name. since the p – value of each of them is greater than 0.05.

Recommendations
It is recommended that MTN Nigeria should put more security on component with high risk impact and other GSM network providers should also carryout risk analysis on their component to find out the component with high vulnerability so that they can increase security of the component. It is also recommended that further research can be carry out on other component of MTN business since this research covers five (5) component of the business.

REFERENCE

1. Dikmen, I., Birgonul, M. T., & Arikan, A. E. (n.d.). A CRITICAL REVIEW OF RISK MANAGEMENT SUPPORT TOOLS, 10.
2. Hasan, Z., Boostanimehr, H., & Bhargava, V. K. (2011). Green Cellular Networks: A Survey, Some Research Issues and Challenges. *ArXiv:1108.5493 [Cs]*. Retrieved from http://arxiv.org/abs/1108.5493
3. Karabacak, B., & Sogukpinar, I. (2005). ISRAM: information security risk analysis method. *Computers & Security*, *24*(2), 147–159. https://doi.org/10.1016/j.cose.2004.07.004
4. Kellermann, T. (n.d.). Mobile Risk Management, 28.
5. Molina, S., Lang, D. H., & Lindholm, C. D. (2010). SELENA – An open-source tool for seismic risk and loss assessment using a logic tree computation procedure. *Computers & Geosciences*, *36*(3), 257–269. https://doi.org/10.1016/j.cageo.2009.07.006
6. Osabutey, E. L. C., & Okoro, C. (2015). Political Risk and Foreign Direct Investment in Africa: The Case of the Nigerian Telecommunications Industry. *Thunderbird International Business Review*, *57*(6), 417–429. https://doi.org/10.1002/tie.21672
7. Seify, M., & Bijani, S. (2009). A Methodology for Mobile Network Security Risk Management. In *2009 Sixth International Conference on Information Technology: New Generations* (pp. 1572–1573). Las Vegas, NV, USA: IEEE. https://doi.org/10.1109/ITNG.2009.321
8. Tran, M. T. N., Tanaka, J., Hamada, M., Sugiyama, Y., Sakaguchi, S., Nakamura, M., ... Miwa, Y. (2014). In Vivo image Analysis Using iRFP Transgenic Mice. *Experimental Animals*, *63*(3), 311–319. https://doi.org/10.1538/expanim.63.311

Computing, Information Systems & Development Informatics Journal
Vol. 9 No. 4, 2018 - www.cisdijournal.org

Security Risk Analysis and Management in Electronic Payment Switching System in Nigeria, eTranzact International Plc. as a Case Study

Ilyas Adeleke Jimoh[1] Joseph A. Ojeniyi[2] & Ismaila Idris[3]
Department of Cyber Security Science
[1,2,3]Federal University of Technology
Minna, Niger State, Nigeria
E-mail: ilyas.pg6757@st.futminna.edu.ng, ojeniyija@futminna.edu.ng, ismi.idris@futminna.edu.ng

ABSTRACT

Security and risk management remain the major challenges of electronic transaction globally. The frequency of usage of at least one of the means of electronic payment system posses a continuous security risk and challenges which may arise as loss of identity in the course of transaction. Loss of any form of payment identity could result into a huge amount of financial loss. Continuous analysis and improving the existing security measures is one of the most effective ways of finding an effective solution to these security risks and challenges being faced in electronic payment and switching industries worldwide. This paper has carefully selected eTranzact International Plc., one of the major payment gateways in Nigeria and x-rayed its components, for the purpose of analysing them and come up with actionable responses to any security risk that may arise. This paper work has extensively reviewed related literature of on the assessment of security risks, related vulnerabilities and management of associated risks with electronic payment system in general. An elaborate questionnaire was designed, administered on the electronic payment system users and carefully analysed. A total of 88 respondents that cut across private, public, informal sectors and students took part in the research. Their responses were therefore analysed using Descriptive statistics to determine strategies that can be adopted in managing security risks that may occur in the process.

Keywords: Information security, risk analysis, risk management, electronic payment and switching system.

CISDI Journal Reference Format
Ilyas Adeleke Jimoh Joseph A. Ojeniyi & Ismaila Idris (2018): Security Risk Analysis and Management in Electronic Payment Switching System in Nigeria, eTranzact International Plc. as a Case Study. Computing, Information Systems & Development Informatics Journal. Vol. 9 No. 4. Pp 15-36- Available online at www.cisdijournal.net

1. INTRODUCTION

In recent years, the electronic payment transactions across the world is estimated at over $34 trillion and in Nigeria, over $425 billion is estimated to be achieved by the end 2018. These financial transactions are being consummated through various electronic payment channels such as mobile payment, NEFT, POS, Web payment etc. annually. Table (a) and figure 1.0 shows the electronic payment financial transactions from Central Bank of Nigeria through various channels. As indicated, in 2016, 70trillion naira was transacted with over 36% increment in 2017, and over 40% increase is expected to be recorded at the end of 2018 (Source, CBN's ePayment Statistics https://www.cbn.gov.ng/Paymentsystem/ePaymentStatistics.asp).

The expansion in volume of financial transaction electronically is creating an alarming vulnerabilities and security threat in the electronic payment gateways. Fraudsters, hackers and crackers are busy exploiting several opportunities ranging from fraudulent sms, to hacking personal information of customers to increase their financial gains through any loose media of electronic payment and electronic commerce channels.

Table a: Electronic Payment Statistics from Central Bank of Nigeria

Channels	2018	2017	2016	2015	2014	2013	2012
Cheques	1,316,890,045,698.70	5,381,909,711,667.16	5,829,549,268,629.00	6,195,461,481,268.00	15,283,933.00	14,211,078.00	12,161,694.00
NEFT	3,869,845,195,383.92	14,946,463,879,672.40	14,584,802,657,086.00	13,087,085,484,769.00	29,690,765.00	29,834,317.00	28,941,559.00
ATM	1,568,949,120,387.82	6,437,592,402,748.64	4,988,133,401,544.00	3,971,651,486,420.00	400,269,140.00	295,416,724.00	375,513,154.00
POS	474,731,342,407.00	1,409,813,091,608.35	758,996,505,702.00	448,512,548,727.00	20,817,423.00	9,418,427.00	2,587,595.00
WEB	60,742,354,767.39	184,596,629,926.57	132,360,333,369.00	91,581,292,533.00	5,567,436.00	2,900,473.00	2,276,464.00
MMO	329,115,761,422.17	1,101,998,974,555.00	756,897,483,653.00	442,353,763,489.00	27,744,797.00	15,930,181.00	2,297,688.00
NIP	17,802,216,863,108.60	56,165,666,312,858.10	38,109,061,203,852.00	25,540,842,563,780.00	40,829,854.00	17,112,158.00	4,449,654.00
EBILLSPAY	125,925,463,535.07	550,750,791,543.15	339,407,748,303.63	217,426,481,827.00	593,579.00	557.00	-
REMITA	5,328,494,109,615.46	13,529,495,515,408.40	10,652,493,933,099.30	6,223,453,782,841.90	15,029,627.00	-	-
NAPS	411,210,891.00	4,960,349,089,466.59	753,689,705,802.99	98,684,511,448.00	-	-	-
M-CASH	1,784,018,273,937.09	616,936,468.57	-	-	-	-	-
CENTRALPAY	2,198,268,367.11	4,996,845,611.06	1,442,064,836.87	311,550,330.00	-	-	-
OVERALL TRANSACTION	**130,654,152,038,085.00**	**104,674,250,181,534.00**	**76,906,834,305,877.80**	**56,317,364,947,432.90**	**555,826,554.00**	**384,823,915.00**	**428,227,808.00**

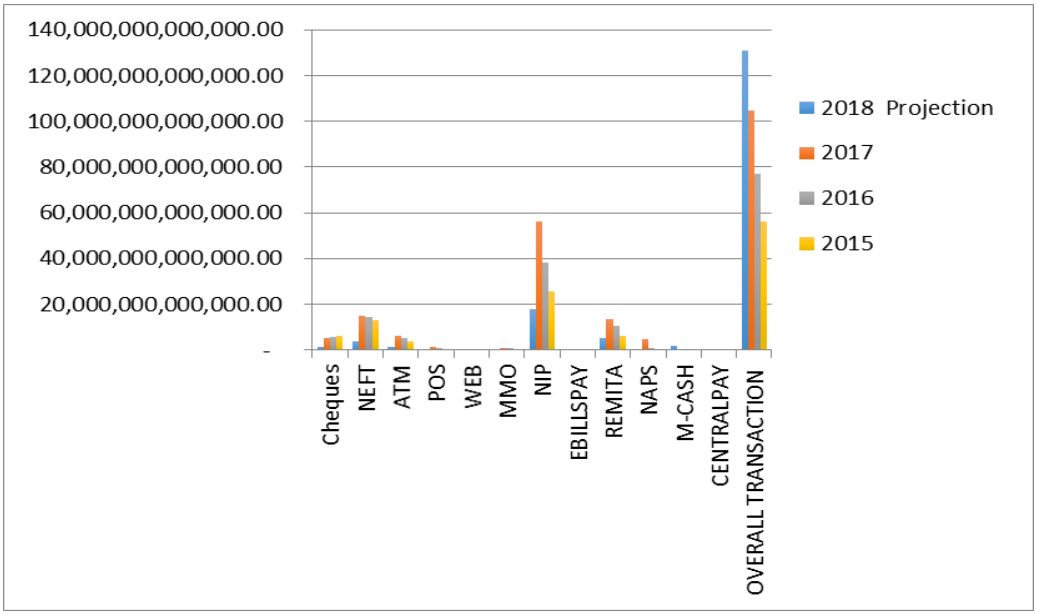

Figure 1.0

1.1 Background of Electronic Payment

The electronic payment, eCormarce, retail payment, government contractual payments, salary payments etc. are various mode of payment which utilises electronic payment infrastructure to achieve a seamless transaction. The payment landscape is shifting increasingly from paper to electronic system as the number of ways and channels to make noncash payments grows. Various electronic payment channels, mobile payment, automated clearing house (ACH), POS payment, ATM and speed-through lanes at toll booths are just a few examples of new payment methods recently introduced to the market. Emerging computing technologies, which gave birth to, online commerce, telecommunications, various other channels of new payment methods rely on electronics for all of their functions. Some products based on these methods did not live long, few managed to develop, while a many have become well-known and accepted in routine transactions and commerce. All of these come a variety of risks. Understanding these risks, several reports of data compromises, identity breaches, and fraud have become an integral part of the electronic payment system gain. Novel characteristics associated with "emerging" payments technologies include low-cost ways to store and transmit transactional data. These technologies therefore reduce risk, but they can also manifest into new risks. Understanding these will convince the payment tech-drivers that the time is now to develop a structure and special strategies for examining how new payment technologies contribute to risk, particularly as the number of ways to make cashless payments channels grows and as payments transform from paper-based to electronic method. Understanding the structure of risk is useful, while assessing losses and mitigation efforts against it in a new payment system should be the major focus.

The ease that an electronic payment and electronic commerce system provide ensures that a large volume of customers will continue to use these systems with growing orders made electronically and delivery carried out with no geographical limitations. These systems enhance normal business flows as now, e-commerce transactions occur as P2P, B2B, B2C, G2C etc. A survey of customer's online shopping habits reveals that more than 5,000 customers will make at least two online purchases within a three-month period. According to this survey, compared with a 47% purchases in 2014 and 48% in 2015, customers now carry out 51% of their purchases online (Affia, 2018). However, the ease introduced by electronic payment and commerce solutions has accompanied by severe cyber threats to the system. Sensitive information is now being generated collected, stored, transmitted, and manipulated on technologies and through processes that may not have adequate security capabilities. Customers now fear the loss of financial data and e-commerce systems fear the financial losses as well as other losses associated with security risks. With these security concerns, a consistent analysis of threats that pose security risks, as well as a continuous process into the treatment of these risks. This paper seeks to provide a structured and logically illustrated approach to continuous threat analysis and security risk management specific to the electronic payment gateway domain. This approach will also facilitate participation between business professionals (who want to participate in a more effective way in building, using and managing e-commerce systems), and the IT professionals (who seek to work more effectively with the business professionals when building and maintaining their e-commerce systems)

2. Objectives of The Study

The major objective of this study is to implement a standard information security system that is devoid of or less prone to threats and vulnerabilities through gathering of customers experience in the usage of various method electronic payment systems. This will enable the management to make a well-informed risk management decisions that will justify expenditures of information security budgets and other information technology systems on the basis of supporting documentation resulting from the performance of risk management (RUSU, 2011).

1.2 Definitions

The Electronic Payment System is simply defined as an Electronic Fund Transfer System (EFT). Electronic funds transfer systems represent a class of transaction driven by computer and data network applications that are categorised by a number of important parameters. These parameters includes but not limited to – very rapid response times, – high reliability and fault tolerance, – widespread distribution of service points and terminals, – large databases, with acceptable levels of complexity, – high levels of confidentiality (privacy), authenticity and integrity, and – terminal operation and interfaces acceptable to the general public. In addition these systems are increasingly becoming the topic of governmental legislation and their impact on the individual is being constantly assessed (Pascal, 1988). Technology advancement and increasing customer sophistication are escalating customer awareness and expectations from businesses hence, demanding more from businesses.

Rapid consumer adoption of non-traditional payment channels, including the internet, Mobile phones, etc. have provided businesses with many new sales, marketing, promotional and other customer interaction opportunities. Activities that the average consumer would perform via brick and mortar branches, kiosks, fax, or mail (e.g. shopping, cash withdrawal, bill payments, statement requests), can now be conducted using the Internet, PDA, ATM, POS, Mobile phone etc, at a much lower cost than with traditional methods. These channels have also proved cost effective in serving the retail market, as it is significantly cheaper than over-the-counter transactions.

In order to leverage the benefits of this trend and ensure sustainable increase in market share, financial services institutions are repositioning through investments in modern tools of technology – including automated payment solutions and rapid deployment of self service terminals.

1.3 Nigeria Electronic Payment Industry Structure

Electronic payment industry is structured in such a way that the Central Bank of Nigeria (CBN) is the regulator, the Nigeria Interbank Settlement System (NIBSS) a subsidiary of CBN coordinates all settlement related activities of all Payment Switching Companies such as eTranzact Plc., Interswitch, Banks etc., while payment methods, transaction processing and users of the electronic payment platforms follows respectively. (Mousley, n.d.).

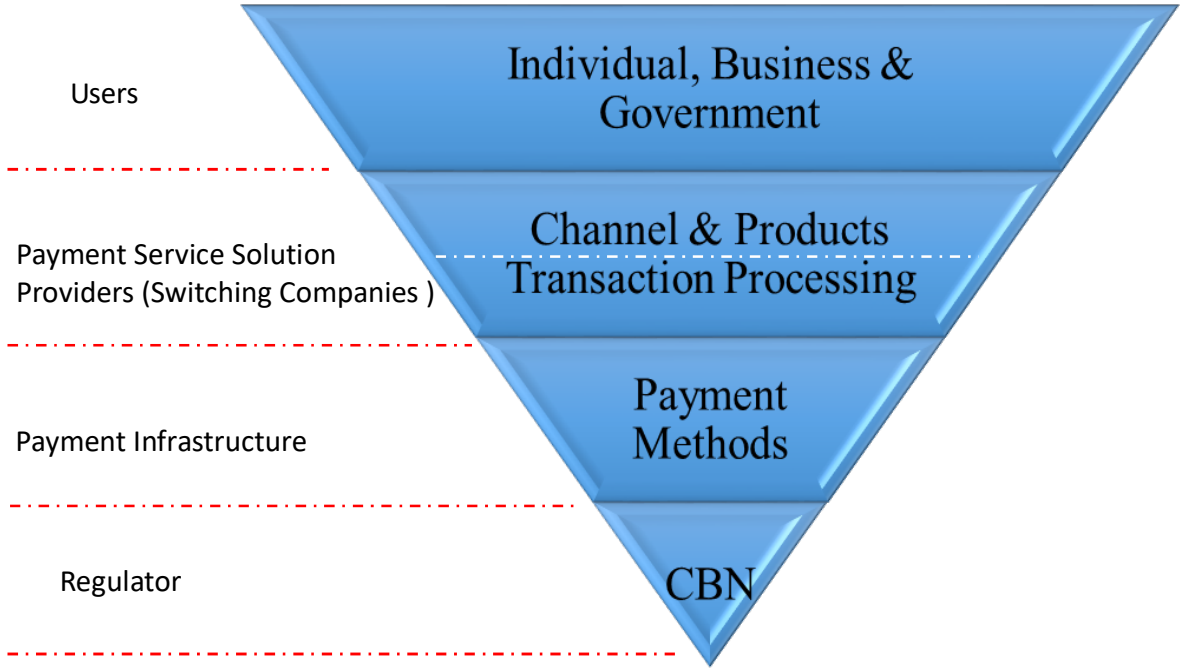

Figure 1.1: Nigeria Electronic Payment Industry Structure (Source: PSV 2020, CBN 2013).

1.4 The Case Study

eTranzact International Plc. deals in electronic payment system such as Internet, POS, and Mobile payment system. The company currently has operations in six other countries around the world; South Africa, Ghana, Zimbabwe, Kenya, Cote d'voire and United Kingdom. Since Inception, eTranzact has deployed its mobile and web payment solutions, to banks and non-bank financial institutions alike and was eTranzact International Plc. is Nigeria's first award winning multi-application and multi-channel electronic transaction switching and payment processing platform. eTranzact has operations in Nigeria, Ghana, Kenya, Zimbabwe, South Africa, Cote d'Ivoire, and UK and is currently expanding operations to more and more countries in the world. ETranzact was launched in September 2003, and has today evolved into a brand with global reach extending its innovative services to include products which cut across virtually all aspects of the e-payment space; ATM, recently granted the license by the Central Bank of Nigeria to provide Mobile Money services to individuals with a special focus on the unbanked sector of the economy. eTranzact has Interswitch Plc., NIBSS Plc., System Specs etc.

2. LITERATURE REVIEW AND RELATED WORK

The world of security risk and management research is a continuous tradition that require consistent and concurrent innovations in order to beat trend of insecurity in third party payment system and other associated e-commerce transaction (Affia, 2018). Introducing security risk management approaches with regard to previous work done on the use of Information System Security Risk Management (ISSRM), STRIDE and DREAD modelling techniques for security risk management are discussed, providing ways of understanding the security need, security threats and the risk management process (Wiley, 2014).

The **ISSRM model** reliance on information systems security risk management and the underlying technologies require a responsible approach to both the technical issues involved as well as the management issues of these underlying structures. Treating IT security not solely as a technical issue but also an all-inclusive approach where interventions are required as governance related, enhances successful implementation of ISSRM model in organizations (Mwambe, 2013). This model is well structured in such away that it can present different concepts and their mutual relationships. The concepts are divided into three major categories; asset related-concepts, risk-related concepts and security-treatment concepts. Threats faced by an information system can be categorized based on the goals and purposes of the attacks. A working knowledge of these categories of threats can help you organize a security strategy so that you have planned responses to threats. **STRIDE** is the acronym used at Microsoft to categorize different threat types and it stand for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. It is a model developed by Microsoft Incp. While **DREAD** model is utilized to figure out the probability of risk, which is abbreviated as Damage Potential, Reproducibility, Exploitability, Affected Users and Discoverability. The threats are rated for a given risk by following the accompanying inquiries (https://www.owasp.org/index.php/Threat_Risk_Modeling).

2.1 The Electronic Fund Transfer Vs Mobile Payment

The rapid growth in the volume and value of financial transactions represents an important source of revenue for the providers of payment service particularly banks, third party payment gateways and other stakeholders (Bank, n.d.). The electronic payment system is majorly, electronic fund transfer, which uses Nigeria Inter-Bank Settlement System (NIBSS) as the backbone. Other forms of it are NEFT, ATM, POS, WEB, MMO, NIP, EBILLSPAY, REMITA, NAPS, M-CASH etc. While Mobile Payment is a form of payment for products or services between two parties for which a mobile device, such as a mobile phone, plays a key role in the realization of the payment. It center on transactions between consumers and merchants that involve direct purchase of goods and services that can be both account-based and point-of-sale (Dahlberg et al., 2011).

2.2 Security and Risk Management In Electronic Payment System

The electronic payment system as an emerging method of payment comes with a challenges such as fraud and other operational problems that exploited its novel characteristics. These incidents include may include but not limited to a telemarketing scheme, a complex online fraud, and two data security breaches. These drawbacks are not necessarily new, but the potential rate and speed of the disruptions are of a magnitude untypical of their paper- based counterparts (Braun, McAndrews, Roberds, & Sullivan, 2008). Some of the related work done in the past analyses type of risks involved such as **telemarketing fraud**. In 2003, the Federal Trade Commission (FTC) announced that it had closed down the Assail Telemarketing Network and its affiliates.

The FTC alleged that the Assail companies ran telemarketing activities from so-called boiler-room operations that offered credit cards to consumers with poor credit records. Under the guise of charging membership fees, these firms persuaded consumers to provide the bank and account information from their checks. The telemarketers then used this information to create electronic debits to consumers' checking accounts as payment for the "membership" fees (Braun et al., 2008). **Transaction Fraud and Data Security Breach** is another kind of security breach that was experienced and reported by the U.S. Department of Justice that, in 2000, two Russian men, Vasiliy Gorshkov and Alexey Ivanov, used unauthorized access to Internet service providers in the United States to misappropriate credit card, bank account, and other personal financial information from more than 50,000 individuals.

They allegedly hijacked computer networks and then used the compromised processors to commit fraud through PayPal and the online auction company eBay (Braun et al., 2008). There was also a research work, which proposes a procedure that targets e-commerce system security and suggests the application of a threat-driven approach to security risk management by analysing an e- commerce system, Webshop as a case study. This approach provides a useful assessment of the security risk management procedure that is validated by experts in the field. It not only identifies evolving threats to e-commerce systems but allows for a structured flow in security risk management(Affia, 2018).

(Hauston, 2017) In his paper proposes a risk management model that can allow universities implement secure information systems. Specifically the paper appraises IS security in the universities and their requirements with a focus on how IS security risks can be managed using ISSRM model. Another white paper examines the current state and nature of the mobile payments market, some of the relevant enabling technologies, looks at the relevant risk, security and assurance issues that security and audit professionals will want to consider when developing and evaluating Electronic Payment System using mobile payment services. (Dahlberg et al., 2011)

Information security measures in electronic payment services should be examined in association with the risk management function to ensure its robustness and effectiveness(European Central Bank, 2014). This implies that variations in the adopted measures should be subject to a formal change management process to ensure that changes are properly planned, examined, documented and authorised. In case any changes executed and security threats noted, there should be a repeated tests on a regular basis and such test should include scenarios of relevant and known potential attacks.

2.2.1 Risk management approach

Risk management can be categorised into 2, namely, the reactive and proactive approach. The reactive approach is most effective when a security incident is occurred. The steps involved in responding to such security incidents are; protecting human life/safety, control damage, damage assessment, causes of the damage, repairing damage and review of responses and update policies. While in proactive risk management approach, rather than wait for a security incident to occur, a preventive measure would have been put in place to avoid such occurrence (RUSU, 2011).

2.2.2 Risk Management Process

In order to ensure a pragmatic risk management process a permanent cycle of process that involves activities for establishing, monitoring and ensuring continual improvement of the organization's activity. Four major activities are involved, design the management system involves identifying business requirements, assessing the likelihood and the impact of the risks, Monitoring, reviewing and reassessing the management system and The improvement and update of the management system (RUSU, 2011).

2.3 Components of An Electronic Payment System

An e-payment system is a method of consummating transactions or making payment for goods and services through an electronic devices, communication media etc, without the use of hardcopy cheques or cash. It is also known as an online payment system. E-Payment system is secure, reliable and seamless method of payment transaction. There is no threat to the user credit card number, smart card or other personal details. The payment can be carried out without involvement of third party, it can also be done at any time through the internet, direct transfer is done through settlement and from E-business environment (Hossein B, 2002).

2.4 The Electronic Payment Ecosystem

The electronic payment system has a wide range of stakeholders. Few of which are listed below: Figure 1.2 below represents the Electronic Payment Eco-system

- Government
- Regulators
- Consumers / Merchants / Users
- Electronic Payment Applications
- Financial service providers (FSPs)
- Payment service providers (PSPs)
- Network service providers (NSPs)
- Device manufacturers
- Regulators
- Standardization and industry bodies
- Trusted service managers (TSMs)
- Application developers

Figure 1.2: Electronic Payment Eco System (Deloitte University Press)

3. RESEARCH METHODOLOGY

We have adopted a qualitative research method where a survey was carried out in private, public, informal sectors, and among few students who are currently using any form of electronic payment such as Mobile, Web, USSD etc. base on reviewed literatures, the researcher was able to understand various mode of payment being sold by eTranzact International Plc. A case study on this project. We have thus used google form to administer a structured questionnaire via internet and through some social media group belonging to some professionals in electronic payment system in Nigeria, technical team of a state where electronic payment was implemented few years back. Total number of 88 valid responses was received and processed using descriptive statistics.

3.1 Results and Data Analysis

Responses were received from questionnaire and extensive investigations were carried out using a descriptive statistic method of data analysis. The following are demographic details of respondents in table 1. The table shows that gender distribution is 79.5% (70 people) are male, 20.5% (18 people) are female. The age classification shows that 21 – 30years of age have 63.6% (56), 31-40 years of age 29.5% (26) while above 40 years of age is 6.8% (6). We have 6.8% (6 respondents) from informal sector, 56.8% (50 people) from private sector, 15.9% (14 people) from public sector, 11.4% (10 respondents) from the undergraduates and 9.1% (8 respondents) from unemployed. Considering the experiences of respondents in terms of years of usage; we have 22.7% (20 people) has been using the ePayment between 0 – 3 years, 33% (29 people) between 4 – 6 years, 25% (22 people) between 7 – 9 years while 19.3 % (17 people) above 10years of usage experience. Also, the analysis shows that 67% (59 people) uses it frequently on a monthly basis, 23.9% (21 people) occasionally use it and 9.1% (8 people) rarely uses it.

Table 1: Demographic Information of Respondents

Alternative	Number	Percentage (%)
Gender		
Male	70	79.5
Female	18	20.5
Total	**88**	**100**
Age		
21-30	56	63.6
31-40	26	29.5
40 and above	6	6.8
Total	**88**	**100**
Sector Status Belong		
Informal Sector	6	6.8
Private Sector	50	56.8
Public Sector	14	15.9
Student Sector	10	11.4
Unemployed	8	9.1
Total	**88**	**100**
Experience with electronic payments		
0-3 years	20	22.7
4-6 years	29	33
7-9 years	22	25
Above 10 years	17	19.3
Total	**88**	**100**
Frequency of usage in a month		
I use it rarely	8	9.1
I use it occasionally	21	23.9
I use it frequently	59	67
Total	**88**	**100**

3.2 Identification and ranking of customer information

This research focuses on identification the risks associated with the electronic payment and information used by customers in the process of financial transaction. To identify various information used by electronic payment system customers, an elaborate literature review was carried out on this topic as it relates to eTranzact International Plc. As a case study. eTranzact is on of the re-known third-party and payment switching providers in Nigeria. Important users' information were identified and itemised, then the respondents were interviewed to rank them according to their order of importance of each information components to the success of the payment, as well as the impact of the information on them. Five point Likert system of ranking was adopted, from Not Important (1), Less Important (2), Neutral (3), Important (4), and Very Important (5). Important information rating as used and indicated by users of electronic payment system are therefore shown in Table 2 below. The customer information column represents all the identified information needed by users to perform financial transactions on the electronic payment platform. The ranking options give the various ranking possibilities of the information based on their importance to the users. The response and percentage columns give the distribution of the respondents in term of number (frequency) and percentage according to the ranking options. For ease of analysis, the ranking option was further categorized into three point Likert option where "Not important "represents "Low impact", "Less important" and "neutral" represent "Medium impact", and "Important" and "Very Important" represent "High impact" respectively.

Table 2: Ranking of Important Information of Electronic Payment Users'

Customer Information Component	Scaling Rate	Responses	Percentage	Impact	Overall scores
Username	Not Important	6	6.8	Low(6)	High
	Less Important	8	9.1	Medium (18)	
	Neutral	10	11.4		
	Important	41	46.6	**High (64)**	
	Very Important	23	26.1		
Login Password	Not Important	3	3.4	Low(3)	High
	Less Important	4	4.5	Medium (5)	
	Neutral	1	1.1		
	Important	13	14.8	**High (80)**	
	Very Important	67	76.1		
Transaction PIN	Not Important	1	1.1	Low (1)	High
	Less Important	1	1.1	Medium (3)	
	Neutral	2	2.3		
	Important	13	14.8	**High (84)**	
	Very Important	71	80.7		
Token	Not Important	6	6.8	Low (6)	High
	Less Important	6	6.8	Medium (19)	
	Neutral	13	14.8		
	Important	23	26.1	**High (63)**	
	Very Important	40	45.5		
Bank Verification Number (BVN)	Not Important	12	13.6	Low (12)	High
	Less Important	16	18.2	Medium (30)	
	Neutral	14	15.9		
	Important	16	18.2	**High (46)**	
	Very Important	30	34.1		

Account Number	Not Important	9	10.2	Low (9)	High
	Less Important	7	8	Medium (15)	
	Neutral	8	9.1		
	Important	28	31.8	**High (64)**	
	Very Important	36	40.9		
ATM Card Number	Not Important	5	5.7	Low (5)	High
	Less Important	4	4.5	Medium (16)	
	Neutral	12	13.6		
	Important	29	33	**High (67)**	
	Very Important	38	43.2		
ATM CVV	Not Important	2	2.3	Low (2)	High
	Less Important	8	9.1		
	Neutral	7	8	Medium (15)	
	Important	27	30.7	**High(71)**	
	Very Important	44	50		
Registered Phone Number	Not Important	6	6.8	Low (6)	High
	Less Important	6	6.8	Medium (10)	
	Neutral	4	4.5		
	Important	33	37.5	**High (72)**	
	Very Important	39	44.3		
Registered E-Mail Address	Not Important	2	2.3	Low (11)	High
	Less Important	9	10.2	Medium (19)	
	Neutral	10	11.4		
	Important	42	47.7	**High(67)**	
	Very Important	25	28.4		
Account Name	Not Important	9	10.2	Low (9)	High
	Less Important	12	13.6	Medium (23)	
	Neutral	11	12.5		
	Important	31	35.2	**High(56)**	
	Very Important	25	28.4		
ATM Card PIN	Not Important	6	6.8	Low (6)	High
	Less Important	5	5.7	Medium (9)	
	Neutral	4	4.5		
	Important	21	23.9	**High (73)**	
	Very Important	52	59.1		
Electronic Receipt	Not Important	5	5.7	Low (5)	High
	Less Important	11	12.5	Medium (26)	
	Neutral	14	15.9		
	Important	31	35.2	**High (58)**	
	Very Important	27	30.7		
E-Mail Password	Not Important	18	20.5	Low (18)	High
	Less Important	10	11.4	Medium (18)	
	Neutral	8	9.1		
	Important	22	25	**High (52)**	
	Very Important	30	34.1		

Further analysis on table 2 shows that electronic payment platform's username, login password, transaction PIN, token, bank verification number (BVN), account number, registered email address, Account name, ATM Card number (PAN), ATM CVV, Registered phone number, ATM Card PIN, electronic receipt and eMail Password are all part of most important customers' information with "High" value impact. Therefore, the distribution of the impact on the Electronic Payment Platform of customers' information is summarized in table 3 below.

Table 3: Impact on the Electronic Payment Users

S/N	Customer Information	Impact
1	Username	High
2	Login Password	High
3	Transaction PIN	High
4	Token	High
5	Bank Verification Number (BVN)	High
6	Account Number	High
7	ATM Card Number	High
8	ATM CVV	High
9	Registered Phone Number	High
10	Registered E-Mail Address	High
11	Account Name	High
12	ATM Card PIN	High
13	Electronic Receipt	High
14	E-Mail Password	High

3.3 Inventory of Technology Adopted

The Inventory of technology used in the implementation of electronic payment system development process is a crucial stage information security system management. This stage enables the security experts to identify the technologies that come in contact with the information uses, stores, processes and transmitted by the electronic payment system during financial transaction. Survey were carried out with the respondents on the technologies (hardware/software), Mobile bank application, internet (web) banking, USSD driven banking, sms based banking, interactive voice response, online transfer (in-bank service), laptop web tokenised banking used for financial transactions (payment) from those that have been pre-identified by the author. Table 4 and figure 2 represent the distribution of the responses from the respondents.

The results show that majority of respondents mostly use mobile phone for electronic payment transaction (88.6%) followed by those that uses mobile phone for Internet banking with 65.9%. It also shows that customers use USSD (Unstructured Supplementary Service Data) for transaction by recording 50%, SMS (short Message Service) based banking 30.7%, while only 6.8% of the respondents use Interactive Voice Response system, Online transfer through bank teller is 47.7% and customers using laptop / desktop with token to perform internet banking are 48.9%.

Table 4: Inventory of Technology Used

S/N	Technology	Response	Percentage (%)
1	Mobile banking application	78	88.6
2	Mobile phone (internet banking)	58	65.9
3	Ussd technology	44	50
4	SMS based banking	27	30.7
5	Interactive voice response	6	6.8
6	Online transfer	42	47.7
7	Laptop (using internet and token)	43	48.9

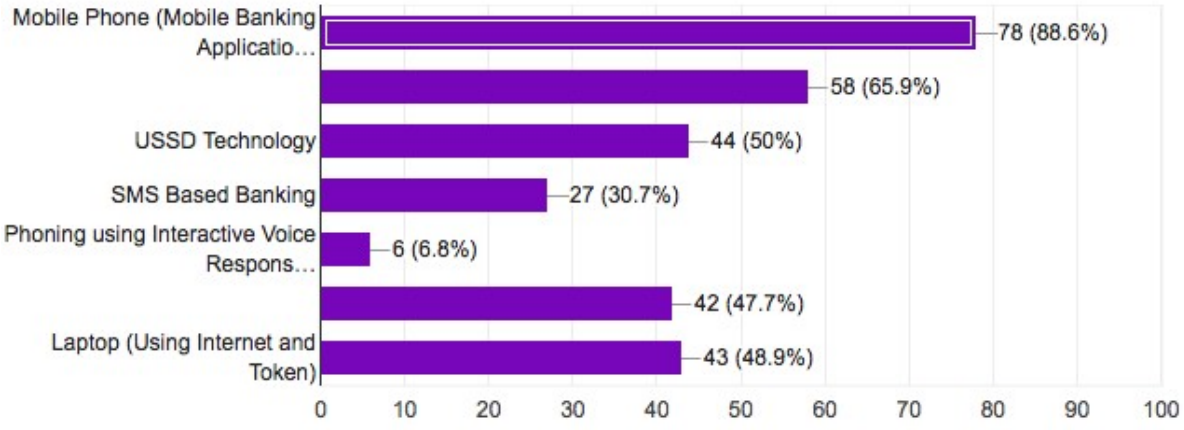

Figure 2: Technology Inventory for electronic payment platform users

3.4 Vulnerability and threat from Electronic Payment Platform Users

In general, users are mostly regarded as the threat link in the information security chain. In order to enhance information security risk management, extra efforts need to be put in place by the electronic payment service providers to avoid threat and vulnerabilities from the users of service which can also constitute threat to the business and users' information. This work has included some information security related questions in this survey in order to assess the vulnerabilities and threats to the security of their information as regards the electronic payment services. Table 5 and figure 3 shows the distribution of responses of the users to the vulnerability and threat related issues from their end.

The results show the probability of the user's information comprised as a result of lost/stolen mobile phone, laptop or other devices is high with respect to 71.6% responses while only 34.1% is of the users installed malicious applications on their devices whether intentionally or accidentally. Some users may disclose their electronic banking details are 37.5%, and those that can Grant device's operating system to modify settings are 55.7% and Electronic devices not available or not connecting to the payment platform is 52.3%. Others are services unavailability from the provider is 51.1%, Network service provider failure is 78.4% and Communication system being tapped by hackers 50%. However, the distribution of the users' responses shows that the vulnerabilities exist from the electronic payment customers and need to be addressed in order to ensure safe electronic payment transaction.

Table 5: Vulnerabilities and threats to Electronic Payment system from customers

S/N	Identification of threat	Response	Percentage (%)
1	Lost / stolen / damaged of Laptop, phone or other devices	63	71.6
2	Installation of malicious app	30	34.1
3	May disclose electronic banking information	33	37.5
4	Grant device's operating system to modify settings	49	55.7
5	Electronic mobile device may not work	46	52.3
6	Services that control functionalities of electronic payment	45	51.1
7	Network service from the telephone	69	78.4
8	Communication system tapped by hackers	44	50

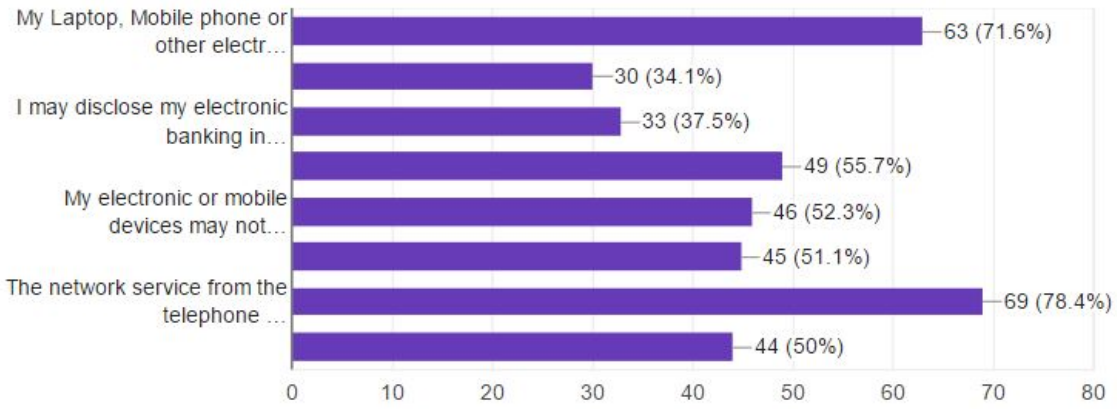

Figure 3: Vulnerabilities and threats to Electronic Payment system from customers

3.5 Vulnerability and Threat from Electronic Payment Service Providers

One of major information system security risk analysis and management procedure is proper understanding of vulnerabilities in electronic payment system as provided by various payment service providers (PSPs). These may pose threats to the confidentiality, integrity, and availability of the customers' information profiles. Therefore, it is very important to determine likelihood of attack on each customer information components and the business system. This will help the management to identify such threat and be able to take an informed security decision. This research work took different security related questions from users of various electronic payment system in this survey. These security questions were based on assessing the possibility of unauthorized access or disclosure (Confidentiality), unauthorized modification (integrity), and the possibility of the failure of the service based on the failure of each of the identified important components of the electronic payment system and users' information. The result of their respective opinion and responses regarding vulnerability and threat to electronic payment platform with respect to the security measures provided by various stakeholders in the eco system is shown in table 6. To analyse the opinion of the electronic payment users on the possibility of attack on their information, we make use of five point Likert options ranging from "Strongly Disagree, Disagree, Neutral, Agree, and Strongly Agree". For the sake of making the analysis easier and more presentable, the author re-categorized the scale into three Likert options where "Low" represents "Strongly Disagree and Disagree", "Medium" represents Neutral and "High" represents "Agree and Strongly Agree",

Table 6: Vulnerability and Threat from Electronic Payment Service Providers

Customer Information Component	Security Properties	Question Options	Response	Percentage	Likelihood	Overall Likelihood
Username	Confidentiality (Possibility of unauthorized access or disclosure)	Strongly Disagree	5	5.7	Low (22)	High
		Disagree	17	19.3		
		Neutral	23	26.1	Medium (23)	
		Agree	27	30.7	**High** (43)	
		Strongly Agree	16	18.2		
	Integrity (possibility of unauthorized modification)	Strongly Disagree	8	9.1		
		Disagree	26	29.5	Low (34)	
		Neutral	13	14.8	Medium (13)	
		Agree	25	28.4	**High** (41)	
		Strongly Agree	16	18.3		
	Availability (possibility of service failure)	Strongly Disagree	5	5.7		
		Disagree	13	14.8	Low (18)	
		Neutral	13	14.8	Medium (13)	
		Agree	36	40.9	**High** (57)	
		Strongly Agree	21	23.9		
Login Password	Confidentiality (possibility of unauthorized access or disclosure)	Strongly Disagree	10	11.4	Low (26)	High
		Disagree	16	18.2		
		Neutral	25	28.4	Medium (25)	
		Agree	26	29.5	**High** (37)	
		Strongly Agree	11	12.5		
	Integrity (possibility of unauthorized modification)	Strongly Disagree	7	8		
		Disagree	21	23.9	Low (28)	
		Neutral	0	0	Medium (0)	
		Agree	36	40.9		
		Strongly Agree	24	27.2	**High** (60)	
	Availability (possibility of service failure)	Strongly Disagree	6	6.8		
		Disagree	14	15.9	Low (20)	
		Neutral	18	20.5	Medium (18)	
		Agree	34	38.6	**High** (50)	
		Strongly Agree	16	18.2		
Transaction PIN	Confidentiality (possibility of unauthorized access or disclosure)	Strongly Disagree	8	9.1		High
		Disagree	17	19.3	Low (25)	
		Neutral	33	37.5	**Medium** (33)	
		Agree	18	20.5	High (30)	
		Strongly Agree	12	13.6		
	Integrity (possibility of unauthorized modification)	Strongly Disagree	10	11.4		
		Disagree	23	26.1	**Low** (33)	
		Neutral	22	25	Medium (22)	
		Agree	21	23.9	**High** (33)	
		Strongly Agree	12	13.6		
	Availability (possibility of service failure)	Strongly Disagree	4	4.5		
		Disagree	13	14.8	Low (17)	
		Neutral	20	22.7	Medium (20)	
		Agree	34	38.6		
		Strongly Agree	17	19.3	**High** (52)	

Account Number	Confidentiality (possibility of unauthorized access or disclosure)	Strongly Disagree	6	6.8	Low (23)	High
		Disagree	17	19.3		
		Neutral	21	23.9	Medium (21)	
		Agree	29	33	**High** (44)	
		Strongly Agree	15	17		
	Integrity (possibility of unauthorized modification)	Strongly Disagree	11	12.5		
		Disagree	20	22.7	**Low** (31)	
		Neutral	28	31.8	Medium (28)	
		Agree	18	20.5	High (29)	
		Strongly Agree	11	12.5		
	Availability (possibility of service failure)	Strongly Disagree	8	9.1		
		Disagree	15	17	Low (23)	
		Neutral	21	23.9	Medium (21)	
		Agree	28	31.8		
		Strongly Agree	16	18.2	**High** (44)	
Electronic Payment BVN	Confidentiality (possibility of unauthorized access or disclosure)	Strongly Disagree	9	10.2	Low (31)	High
		Disagree	22	25		
		Neutral	21	23.9	Medium (21)	
		Agree	21	23.9	**High** (36)	
		Strongly Agree	15	17		
	Integrity (possibility of unauthorized modification)	Strongly Disagree	11	12.5		
		Disagree	27	30.7	**Low** (38)	
		Neutral	21	23.9	Medium (21)	
		Agree	17	19.3	High (29)	
		Strongly Agree	12	13.6		
	Availability (possibility of service failure)	Strongly Disagree	8	9.1		
		Disagree	21	23.9	Low (29)	
		Neutral	19	21.6	Medium (19)	
		Agree	22	25	**High** (40)	
		Strongly Agree	18	20.5		
Registered Phone numbers	Confidentiality (Possibility of unauthorized access or disclosure)	Strongly Disagree	8	9.1	Low (23)	High
		Disagree	15	17		
		Neutral	18	20.5	Medium (18)	
		Agree	34	38.6	**High** (46)	
		Strongly Agree	12	14.8		
	Integrity (possibility of unauthorized modification)	Strongly Disagree	9	10.2		
		Disagree	21	23.9	Low (30)	
		Neutral	18	20.5	Medium (18)	
		Agree	25	28.4		
		Strongly Agree	15	17	**High** (40)	
	Availability (possibility of service failure)	Strongly Disagree	5	5.7		
		Disagree	23	26.1	Low (28)	
		Neutral	18	20.5	Medium (18)	
		Agree	27	30.7		
		Strongly Agree	15	17	**High** (42)	

Registered E-mail Address	Confidentiality (Possibility of unauthorized access or disclosure)	Strongly Disagree	8	9.1	Low (21)	High
		Disagree	13	14.8		
		Neutral	25	28.4	Medium (25)	
		Agree	27	30.7	**High** (42)	
		Strongly Agree	15	17		
	Integrity (possibility of unauthorized modification)	Strongly Disagree	10	11.4		
		Disagree	17	19.3	Low (27)	
		Neutral	29	33	Medium (29)	
		Agree	19	21.6		
		Strongly Agree	13	14.8	**High** (32)	
	Availability (possibility of service failure)	Strongly Disagree	9	10		
		Disagree	20	22.7	Low (29)	
		Neutral	26	29.5	Medium (26)	
		Agree	16	18.2	**High** (33)	
		Strongly Agree	17	19.3		
Registered E-mail Address Password	Confidentiality (Possibility of unauthorized access or disclosure)	Strongly Disagree	11	12.5	Low (32)	High
		Disagree	21	23.9		
		Neutral	22	25	Medium (22)	
		Agree	19	21.6	**High** (34)	
		Strongly Agree	15	17		
	Integrity (possibility of unauthorized modification)	Strongly Disagree	10	11.4		
		Disagree	21	23.9	Low (21)	
		Neutral	28	31.8	Medium (28)	
		Agree	15	17		
		Strongly Agree	14	15.9	**High** (29)	
	Availability (possibility of service failure)	Strongly Disagree	10	11.4		
		Disagree	18	20.5	Low (28)	
		Neutral	29	33	Medium (29)	
		Agree	15	17		
		Strongly Agree	16	18.2	**High** (31)	
ATM Card Number	Confidentiality (Possibility of unauthorized access or disclosure)	Strongly Disagree	9	10.2	Low (26)	High
		Disagree	17	19.3		
		Neutral	26	29.5	Medium (26)	
		Agree	22	25	**High** (36)	
		Strongly Agree	14	15.9		
	Integrity (possibility of unauthorized modification)	Strongly Disagree	12	13.8		
		Disagree	21	23.9	Low (33)	
		Neutral	19	21.6	Medium (19)	
		Agree	23	26.1	**High** (36)	
		Strongly Agree	13	14.8		
	Availability (possibility of service failure)	Strongly Disagree	7	8		
		Disagree	17	19.3	Low (24)	
		Neutral	22	25	Medium (22)	
		Agree	26	29.5		
		Strongly Agree	16	18.2	**High** (42)	
	Confidentiality (Possibility of unauthorized access or disclosure)	Strongly Disagree	8	9.1	Low (24)	
		Disagree	16	18.2		
		Neutral	21	23.9	Medium (21)	
		Agree	24	27.3	**High** (43)	
		Strongly Agree	19	21.6		
	Integrity	Strongly Disagree	12	13.6		

Bank Account Name	(possibility of unauthorized modification)	Disagree	21	23.9	**Low** (33)	**High**
		Neutral	22	25	Medium (22)	
		Agree	21	23.9		
		Strongly Agree	12	13.6	**High** (33)	
	Availability (possibility of service failure)	Strongly Disagree	10	11.4		
		Disagree	20	22.7		
		Neutral	26	29.5		
		Agree	18	20.5		
		Strongly Agree	14	15.9		
ATM Card CVV	Confidentiality (Possibility of unauthorized access or disclosure)	Strongly Disagree	7	8	Low (23)	**High**
		Disagree	16	18.2		
		Neutral	27	30.7	Medium (27)	
		Agree	21	23.9		
		Strongly Agree	17	19.3	**High** (38)	
	Integrity (possibility of unauthorized modification)	Strongly Disagree	8	9.1		
		Disagree	25	28.4	**Low** (33)	
		Neutral	24	27.3	Medium (24)	
		Agree	18	20.5		
		Strongly Agree	13	14.8	High (31)	
	Availability (possibility of service failure)	Strongly Disagree	8	9.1		
		Disagree	21	23.9	Low (29)	
		Neutral	22	25	Medium 22	
		Agree	22	25		
		Strongly Agree	15	17	**High** (37)	
ATM Card PIN	Confidentiality (possibility of unauthorized access or disclosure)	Strongly Disagree	5	5.7	Low (31)	**High**
		Disagree	26	29.5		
		Neutral	23	26.1	Medium (23)	
		Agree	19	21.6	**High** (34)	
		Strongly Agree	15	17		
	Integrity (possibility of unauthorized modification)	Strongly Disagree	8	9.1		
		Disagree	23	26.1	Low (31)	
		Neutral	22	25	Medium (22)	
		Agree	21	23.9		
		Strongly Agree	14	15.9	**High** (35)	
	Availability (possibility of service failure)	Strongly Disagree	7	8		
		Disagree	13	14.8	Low (20)	
		Neutral	25	28.4	Medium (25)	
		Agree	27	30.7		
		Strongly Agree	16	18.2	**High** (43)	
Transaction Token (OTP)	Confidentiality (possibility of unauthorized access or disclosure)	Strongly Disagree	11	12.5	Low (28)	
		Disagree	17	19.3		
		Neutral	25	28.4	Medium (25)	
		Agree	21	23.9	**High** (35)	
		Strongly Agree	14	15.9		
	Integrity (possibility of unauthorized modification)	Strongly Disagree	13	14.8		
		Disagree	18	20.5	Low (31)	
		Neutral	24	27.3	Medium (24)	
		Agree	20	22.7	**High** (33)	
		Strongly Agree	13	14.8		
	Availability (possibility of	Strongly Disagree	6	6.8		
		Disagree	16	18.2	Low (22)	

	service failure)	Neutral	25	28.4	Medium (25)	**High**
		Agree	24	27.3		
		Strongly Agree	17	19.3	**High** (41)	
Transaction e-receipt	Confidentiality (possibility of unauthorized access or disclosure)	Strongly Disagree	7	8	Low (24)	**High**
		Disagree	17	19.3		
		Neutral	30	34.1	Medium (30)	
		Agree	22	25	**High** (33)	
		Strongly Agree	12	13.6		
	Integrity (possibility of unauthorized modification)	Strongly Disagree	7	8		
		Disagree	19	21.6	Low (26)	
		Neutral	28	31.8	Medium (28)	
		Agree	23	26.1		
		Strongly Agree	11	12.5	**High** (34)	
	Availability (possibility of service failure)	Strongly Disagree	7	8		
		Disagree	19	21.6	Low (26)	
		Neutral	25	28.4	Medium (25)	
		Agree	25	28.4		
		Strongly Agree	12	13.6	**High** (37)	

From Table 6 above, it was observed that all users' information components are important and are marked "High" value or impact. Table 7 below therefore summarises the likelihood attack on the users' information components.

Table 7: Summary of the impact of the Electronic Payment Platform User information

S/N	Electronic Payment Platform (Users Information)	Attack Likelihood
1.	Username	High
2.	Login Password	High
3.	Transaction PIN	High
4.	Bank Account No	High
5.	Electronic Payment BVN	High
6.	Registered Phone No	High
7.	Registered EMail Address	High
8.	Registered EMail Address Password	High
9.	Account Name	High
10.	ATM Card No.	High
11.	ATM Card CVV	High
12.	ATM Card PIN	High
13.	Transaction Token (OTP)	High
14.	Transaction e-receipt	High

3.6 Prioritizing the Information Security System Resolution Action

The concluding phase of information security system and risk management process as recommended by the National Institute of Standards and Technology (NIST) and described by (Paulsen & Toth, 2016)is to combine the impact of identified information components with the likelihood of security incidents, in order to help organization and business executives to determine the information security decision needed to secure users information and their information systems. Securing every aspect of business information with the same level of security may not be feasible as it might be too expensive for the business. Therefore, a need for prioritizing the security efforts is highly important.

The table 8 below shows the priority level that determines the security efforts needed to ensure security and privacy of the Electronic Payment users based on the combination of the impact and the likelihood. Each priority level also indicates various processes and tools the businesses need to consider to protect the information and information systems based on the cyber security framework.

Table 8: Prioritize resolution action

Impact	**High**	Priority 5	Priority 2	Priority 1
	Medium	Priority 7	Priority 4	Priority 3
	Low	Priority 0: No action needed	Priority 8	Priority 6
		Low	**Medium**	**High**
		Likelihood		

Source: Adapted from (Paulsen & Toth, 2016) and modified by the author

3.7 Interpretation of Impact and Likelihood Priority Level

- **Priority 1:** This level requires that the Electronic Payment service provider should implement an **"immediate"** security resolution that can **"detect"** and **"protect"** customers' information and the entire information systems from any security incident.
- **Priority 2:** it requires that the Electronic Payment service provider should implement an **"immediate"** security resolution that can **"detect"** and **"protect"** customers' information and the entire information systems from any security incident.
- **Priority 3:** This requires that the Electronic Payment service providers should **"schedule"** a security resolution that can **"detect"** and **"protect"** customers' information and the entire information systems from any security incident.
- **Priority 4:** This requires that the Electronic Payment service providers should **"schedule"** a security resolution that can **"detect"** and **"protect"** customers' information and the entire information systems from any security incident.
- **Priority 5:** This requires that the Electronic Payment service providers should **"schedule"** a security resolution that can **"Respond"** and **"Recover"** customers' information and the entire information systems from any security incident.
- **Priority 6:** This requires that the Electronic Payment service providers should **"schedule"** a security resolution that can **"Respond"** and **"Recover"** customers' information and the entire information systems from any security incident.
- **Priority 7:** This requires that the Electronic Payment service providers should **"schedule"** a security resolution that can **"Respond"** and **"Recover"** customers' information and the entire information systems from any security incident.
- **Priority 8:** This requires that the Electronic Payment service providers should **"schedule"** a security resolution that can **"Respond"** and **"Recover"** customers' information and the entire information systems from any security incident.
- **Priority 0:** This requires no serious action to be implemented or scheduled from the information security professional

Therefore, from the prioritize resolution action in table 8 above, we can derive and recommends prioritized security action and efforts needed by the electronic payment system service providers in order to ensure security and privacy of customers' information components, based on the results of the analysis of the responses from our respondents. This is summarised in table 9.

Table 9: Prioritized security action needed by the electronic payment system service providers

S/N	Customer Information	Impact	Likelihood of Attack	Priority Level
1	Username	High	High	Priority 1
2	Login Password	High	High	Priority 1
3	Transaction PIN	High	High	Priority 1
4	Token	High	High	Priority 1
5	Bank Verification Number (BVN)	High	High	Priority 1
6	Account Number	High	High	Priority 1
7	ATM Card Number	High	High	Priority 1
8	ATM CVV	High	High	Priority 1
9	Registered Phone Number	High	High	Priority 1
10	Registered E-Mail Address	High	High	Priority 1
11	Account Name	High	High	Priority 1
12	ATM Card PIN	High	High	Priority 1
13	Electronic Receipt	High	High	Priority 1
14	E-Mail Password	High	High	Priority 1

4. CONCLUSION

The electronic payment switching technology is one of the most demanding technologies in the world today. The increasing volume of transactions on a daily basis is a major source of security concern to the stakeholders. This however, requires a strategic security attention due to the volatility of the customer information components. This research work have carefully gathered customers opinions based on the common customer information components that are constantly being used in the process of financial transactions. The tools and media, which the financial transaction comes in contact with in the process, are also key factors that determine the security of such information. In carrying out this work, it was revealed that continuous security risk assessments and analysis would ensure a proactive security decisions to be carried out in a well-defined manner through a collaborative approach of the business stakeholders. Although eTranzact International Plc. was used as a case study, all other payment service provider can adopt the submission on this research work to respond to any security incident occurrence at any point in time. The future research work direction should look at using inferential statistics as a tool for analysing data collected in the course of data gathering. It should also look at possibility of combining many electronic payment service providers in consideration of their respective products, to provide a more elaborate solution to the research problem. This will provide a more elaborate strategy in response to incidents as a result of vulnerabilities that might have been explored to create a security incident/attack.

5. RECOMMENDATION

Electronic payment system is one of the major means of financial transactions worldwide. The concentrations of users in its adoption as a fastest means of performing financial transaction make it more prone to security risks. This research work has holistically analysed and proffers security response solution to it. It is therefore recommended that the users and the service providers cooperate to ensure proper implementation of necessary security procedure to avoid incident occurrences.

REFERENCES

1. Affia, A. O. (2018). Security Risk Management of E-commerce Systems.
2. Bank, C. (n.d.). NIGERIAN PAYMENTS SYSTEM RISK AND INFORMATION SECURITY MANAGEMENT FRAMEWORK.
3. Braun, M., McAndrews, J. J., Roberds, W., & Sullivan, R. J. (2008). Understanding risk management in emerging retail payments. *Economic Policy Review*, *14*(2), 137–159.
4. Dahlberg, T., Mallat, N., Öörni, A., Communication, N. F., Aditya, P., Technology, E., ... Mitchell, C. J. (2011). The concept of security and trust in electronic payments. *Computers and Security*, *24*(1), 75–81. https://doi.org/10.1016/j.cose.2004.11.001
5. European Central Bank. (2014). *Assessment guide for the security of internet payments*. Retrieved from http://bookshop.europa.eu/uri?target=EUB:NOTICE:QB0414051:EN:HTML%5Cnhttps://www.ecb.europa.eu/pub/pdf/other/assessmentguidesecurityinternetpayments201402en.pdf?1cb42bdb72f4c5ef75ec637e59a0bfda
6. Hauston, B. dan. (2017). Teil 2 1. *Main*, *5*(June), 16–59. https://doi.org/10.1093/gji/ggy229/5040233
7. Mousley, P. (n.d.). Financial System Strategy SMEs – The Issues, 1–15.
8. Mwambe, O. O. (2013). Syntactic and Semantic Extensions of Malicious Activity Diagrams to Support ISSRM, *67*(4), 33–39.
9. Pascal, T. (1988). AUSTRALIAN COMPUTER Bob Wallace on what he does and doesn ' t.
10. Paulsen, C., & Toth, P. (2016). *Small Business Information Security: The Fundamentals*. https://doi.org/10.6028/NIST.IR.7621r1
11. RUSU, E. R. S.—A. C. (2011). Security Risk Management - Approaches and Methodology. *Informatica Economica Journal*, *15*(1), 228–240.