



SMART SOCIETY FOR MULTIDISCIPLINARY AND ADVANCED RESEARCH TECHNIQUES



In collaboration with
THE DEPARTMENT OF OPERATIONS AND MANAGEMENT INFORMATION SYSTEM
UNIVERSITY OF GHANA

International Science, Technology, Education, Arts, Management and Social Sciences (iSTEAMS) Conference

An Inter-tertiary and Multidisciplinary Institution Based Conference

13th iSTEAMS Conference

Venue:
Balme Library,
University of Ghana
Legon, Accra, Ghana.



Journal Research Series

SERIES 13



ref member

**WEDNESDAY 24TH - FRIDAY 26TH
OCTOBER, 2018.**

Theme:

**ADDRESSING HUMAN-CENTRED
CHALLENGES THROUGH
MULTIDISCIPLINARY
INNOVATIONS AND INTER-TERTIARY
COLLABORATION**

Editors

PROF. LONGE OLUMIDE BABATOPE

*Multidisciplinary & Cyber Systems Research Group
ICITD, Southern University, Baton Rouge, LA, USA*

DANQUAH PAUL ASANTE (PhD)

Heritage University College, Ghana, Accra Ghana

PROF. ADEKUNLE OKUNOYE

Xavier University, Cincinnati, Ohio USA

PROF. RICHARD BOATENG

University of Ghana, Legon, Ghana



Proceedings of the ISTEAMS Multidisciplinary Cross-Border Conference
University of Ghana, Legon, October, 2018.

Book of Proceedings

SERIES 13

Society for Multidisciplinary & Advanced Research Techniques (SMART)

In Collaboration with the
Department of Operations and Management Information Systems
University of Ghana, Legon

**The 13th SMART-iSTEAMS
International Multidisciplinary Conference Series**

24th - 26th October, 2018

Held at
The Balme Library
University of Ghana
Legon, Accra, Ghana

www.isteam.net
info@isteam.net

© 2018



ACKNOWLEDGEMENT

The 13th iSTEAMS Conference Committee for the 2018 iSTEAMS Conference at the University of Ghana gratefully acknowledge the contributions of all organizations, institutions and individuals who contributed through various means to the success of the Conference. A very special appreciation to the Department of Operations & MIS, University of Ghana for collaborating with SMART to run and participate in the Conference.

COPYRIGHT & REPRINT POLICY

This Book of Proceedings contains peer-reviewed papers presented during the University of Ghana International Multidisciplinary Conference 13th iSTEAMS Conference Series. They reflect the opinion of the authors and their inclusion in the Book of Proceedings does not constitute the endorsement of the Conference Program Committee, the Organizers and the collaborating institutions. Abstracting and content usage within the limit of acceptable use standards are permitted with credit to the source(s). Libraries may photocopy the articles in this proceeding for academic and educational/research purposes. Copying of individual articles for non-commercial purposes is permitted without a fee, provided that credit to the source is given.

Authors **RETAIN** the copyright and all liabilities for their article(s). For other form of copying, reprint, duplication or re-publication purposes, permission from the authors should be obtained in writing.

For all enquiries on the iSTEAMS/SMART Conferences and other information please contact the Programme Committee using the contact details below:

E-mail - info@isteam.net

Phone: +2348160900893
+2348024071175
+2348154413298
+2348061364681



Proceedings Articles' Authorship, Title & Pagination

- Akinbols, B.R.
Asphyxiating Impediments In Access To Equal Right To Education For Persons With Disabilities In Africa
Pp 1-6
- S.O. Salawu
Transient Analysis of Radiative Hydromagnetic Poiseuille fluid flow of Two-step Exothermic Chemical Reaction through a Porous Channel with Convective Cooling.
Pp 7-18
- D.O. Ajala, J.O. Fasakin & O.A. Ajala
Information & Communication Technology: A stranger in the Urban Planning Practice - Findings and Reflections on Osogbo
Pp 19-26
- Emmanuel H. Gadzama, Olawale S. Adebayo, Joseph A. Ojeniyi & Shafi M. Abdulhamid
Risk Analysis and Management in Airline Transportation Using Jumia Air Travel as a Case Study.
Pp 27-50.
- Makanjuola Emmanuel Ayokunnu
Emotional Intelligence and Emotional Labour as Determinants of Organisational Commitment.
Pp 49-60.
- Ajayi, Ibinke Adetolu & Omolore, Olatomide Bamidele
Evaluation of the Wound Healing Activity of Mangifera indica Seed Extract in Wistar Rats.
Pp 61-78
- Lawrence Odey Olong
"Animal Right": A Challenge for African Ethics.
Pp 79-86.
- C. Oslm, Ndifon
The Power of the Ballot and the Role of Tertiary Institutions in the Shaping of Nigeria's Democracy.
Pp 95-100
- Ilesanmi Stephen Idowu
Customary Law, the Environment and Sustainable Development.
Pp 100-106
- Mary Julius Egbai & Chukwueloka S. Uduagwu
Ecofeminism and Political Communication: A Philosophical Assessment of Wangari Maathai's Contribution.
Pp 107-114
- Mary Julius Egbai & Chukwueloka S. Uduagwu
Individuals Internet Security Perceptions and Behaviors: Polycontextual Contrast Between Ghana And Nigeria..
Pp 115-118
- Samuel Anim-Yeboah & Prof. Richard Boateng
Conceptualizing Digital Technologies and Digital Entrepreneurship: Evidence from a Developing Country.
Pp 119-126
- Bibi Dzifa Tomiwa
Where Are We On Information Infrastructure? - A Systematic Literature Review.
Pp 127-128
- Eunice Yeboah Afeti
Cultural Influence on Drivers and Barriers to Merchant Adoption of Mobile Payments
Pp 130-134



Proceedings Articles' Authorship, Title & Pagination

Kwame Simpe Ofori
Exploring Mobile SNS Continuance Intention from the Perspective of Network Externalities and Mobile Value.
Pp 135-145

Klaus vonBuckstein & Richard Boateng
Evaluating the Design of Local Government E-Government Systems – A Human Centred Design Approach.
Pp 146

Mansah Preko & Richard Boateng
Health Informatics and Brain Drain Mitigation in Developing Countries – A Case of Ghana
Pp 147-152

Mansah Preko & John Effah
ICT Innovation Maturity in The Public Sector
Pp 153-158

Muhammad Najmudeen Adouli & Richard Boateng
Assessment of Data Quality and Information Use of District Health Information Systems (DHIS2) in a Developing Country: The Case of Ghana
Pp 159-166

~~Yara Adenomon Taiwo~~
Combating Counterfeiting and Piracy in the Fashion and Beauty Industry in Ghana: The Role of Information Technology.
Pp 167-174



~~Umaru Usman Alhassan~~
Use of Smart Phone Skills and Effective Teaching in Faculty Of Education, University Of Calabar, Nigeria.
Pp 175-178

Peace Eburulowa Kulawo, Sunday Festus Olosupo & Rafiu Oyesola Salawu
Adoption of International Financial Reporting Standards (IFRS) And Quality Of The Central Bank Of Nigeria (CBN) Financial Reports.
Pp 179-184

Edward E. Ogheneovo
Software Evolution: Improving the Quality and Maintainability of Software.
Pp 185-194

Ikotun, S.I & Adigun, T.
Strategic Marketing Planning And Customer Satisfaction: A Perspective For Sustainable Development Of Deposit Money Banks in Nigeria
Pp 195-216

Oga, R.O., Egbokhare, F.A & Obaniagbon, K.O.
Business Process Analysis: A Precursor to Software Cost Estimation in Software Development Projects
Pp 217 -224

Oluwatunde, S; Johnson, Agbesawa, D.O. , Ogunjimi, L.A. & Longe, O.B
Evaluation Of Nigeiran Mobile Network Inference Using Residue Number System
Pp 225 -234

Aderle B.J, Onafu, F., Alashin O.A. Adesokun K.G. & Adesokun A.A.
Evaluation of Electrical Power Outages: A Restructuring Approach in Nigeria.
Pp 235 -244.

Amos Iyole
Autosegmental Analysis of Consonant Deletion of Ijebu-French Bilinguals in Selected Universities in South West of Nigeria. Vol. 2
Pp 245



Risk Analysis and Management in Airline Transportation Using Jumia Air Travel as a Case Study

Emmanuel H. Gadzama, Olawale S. Adebayo, Joseph A. Ojeniyi & Shafii M. Abdulhamid
Department of Cyber Security
Federal University of Technology
Minna, Nigeria
Phone: +234-8126980414
E-mail: ehgadzama@gmail.com

ABSTRACT

An understanding of the risk nature of the airline industry is important in effectively managing the business. The purpose of a risk assessment is to make a decision whether the risk of a given situation is within an acceptable range, and, if not, how we can reduce it to a tolerable level. Security risk in the airline transportation attracts keen focus because of the expansion of differing cyber-attacks; many being inspired by technology improvement. Transportation safety specifically the identification, valuation, and reduction of risks to the massive transportation system, has expanded greatly, experiencing great change and challenge along the way. This paper examined risk analysis and management in airline transportation using jumia air travel as a case study. Recommendations were made based on our findings.

Keywords: Risk Analysis, Management, Airline, Transportation, Jumia Air Travel and Case Study

ISTEAMS Cross-Border Conference Proceedings Paper Citation Format

Emmanuel H. Gadzama, Olawale S. Adebayo, Joseph A. Ojeniyi & Shafii M. Abdulhamid (2018). Risk Analysis and Management in Airline Transportation Using Jumia Air Travel as a Case Study. Proceedings of the 13th ISTEAMS Multidisciplinary Conference, University of Ghana, Legon, Accra, Ghana. Vol. 2, Pp 27-50.

INTRODUCTION

There are many interpretations regarding the meaning of risk and how to manage it. The origin of the word risk is *risicare*, which is an early Italian word for dare (Bernstein, 1996). In the seventeenth century the study of risk began and was in the initial stage linked to trying to apply mathematics to gambling (Frosdick, 1997). These early studies led to the development of probability theory, which is a key factor in the concept of risk (Bernstein, 1996). Associated with gambling for many years, during the early nineteenth century, the term risk was adopted by the insurance industry in England (Moore, 1983).

According to Moore (1983) there are two basic components of risk: (1) risk as a future outcome and (2) the probability that a particular outcome may occur. Risk has both a positive and negative side to it, both the possibility of loss and the hope of gain (Moore, 1983). However, previous studies have shown that organisations seem to focus more on the negative aspects concerning their day-to-day (Hood & Young, 2005; March & Shapira, 1987). Risk management is considered a general management function that seeks to assess and address risk in the organisation as a whole (Fone & Young, 2000).

According to Cox and Townsend (1998), the process of risk management begins by evaluating two factors: (1) the likelihood of specific events occurring and (2) the consequences, if it actually occurs. Smallman (1996) argues that effective risk management should be based on good common sense, rather than highly formalised and structured processes. Risk could be said to be a function of threats, vulnerabilities, the likelihood of an event, and the potential impact such an event would have to the business. Security risk analysis is essential to the security of any organization. Most businesses face information security and cybersecurity threats and vulnerabilities. Whereas certain categories of threats and vulnerabilities may be consistent across businesses, some may be specific to your industry, location, and business.



You should regularly review what threats and vulnerabilities your business may face and estimate the likelihood that you will be affected by that threat or vulnerability. This can assist you identify specific strategies to protect against that threat or vulnerability. Currently, there is lack of cyber security best practices in the Jumia Air Travel. This situation has made it difficult for the Organisation to effectively analyse and manage its security risks. Thus, with the evolution of technology and the increasing dependency on information technology, there was a need for the Jumia Air Travel to implement security risk measures.

During the study, the following research questions were answered: What would happen if customers' information was made public? What would happen if customers' information was incorrect? What would happen if customers couldn't access their information? What strategies can be employed to mitigate risks facing the Jumia Air Travel?

This paper offers a perspective on security risk analysis and management in airline transportation using Jumia Air Travel as a case study. The result of this paper provides knowledge about the usefulness of security risk analysis and thus, assists the Jumia Air Travels to be proactive in terms of managing both targeted and pervasive risks. The study would also encourage Jumia Air Travel management develop appropriate security risk policies, standards, guidelines and better understand the security risks facing their Organisation.

2. RELATED WORKS

This Section presents the review of related work carried out for the purpose of the study. Security risk models on situational awareness for security risk management, systematic risk, airline service quality, air transportation security as well as paradox rule by experts were studied and summarized in terms of gaps that the proposed paper is aiming to address.

Webb, Ahmad, Maynard and Shanks (2014) developed a Situation Awareness Model for Information Security Risk Management (ISRM). The model discourses shortfalls in the practice of information security risk assessment that certainly led to poor decision-making and insufficient or inapt security policies. The three deficiencies are: 1) information security risk identification is commonly perfunctory, 2) information security risks are commonly estimated with little reference to the organization's actual situation and 3) information security risk assessment is commonly performed on an sporadic, non-historical basis. The deficiencies were not properly addressed. Hence, there is need to address the deficiencies through an enterprise-wide collection, analysis and reporting of risk related information. The systematic risk research was based on the CAPM as defined by Lintner (1965) and Sharpe (1963, 1964). The CAPM suggests that the expected rate of return on a risk asset can be obtained by adding risk-premium to risk-free rate, and the expected risk premium varies in direct proportion to beta in a competitive market (Chen, 2003; Gencay, Selcuk, & Whitcher, 2003; Lintner, 1965; Sharpe, 1963, 1964; Sheel, 1995).

Additionally, the study conducted another multiple regression analysis. The analysis was intended to examine what factors under management control influence total risk. It would allow better understanding of the company specific variables by comparing their relationships to systematic risk and total risk. This study focused on the relationships between firm specific variables and systematic risk. Results indicated that debt leverage, profitability, firm size, growth, and safety were found to be significant predictors of systematic risk in the US airline industry whereas the rest of variables including liquidity and operating efficiency were not found to be significantly related to the systematic risk. The findings of this study suggested that the systematic risk was significantly related to some firm-specific characteristics. To disclose more fine-grained relationship between factors under management's control and risk, future research was advised to include more firm-specific variables such as stock turnover ratio and earning dividend ranking (BenZion & Shalit, 1975). This would help enhance more practical implications and capture various aspects on the risk-management policy linkage.

Studies that have addressed service quality topics in the airline industry have explored and measured service attributes, including studies by Robledo (2001), Park et al. (2004, 2006), Chen and Chang (2005), and An and Noh (2009). Rhoades and Waguespack Jr. (2008) reviewed the conceptual foundations for service quality as it applied to the airline industry, and used data from the Air Travel Consumer Report to investigate airline quality performance regarding such key indicators as on-time arrivals, customer complaints, denials of boarding, and occurrences of mishandled baggage to characterize trends in airline service performance over the last two decades. Saha and Theingi (2009) indicated that, regarding order of priority, the dimensions of service quality, in descending order, are flight schedules, flight attendants, tangibles, and ground staff. Curry and Gao (2012) examined relationships among service quality, service satisfaction, and customer loyalty in a budget airline.



Descriptive statistics (frequencies) was used to analyze the responses in MS Excel. SPSS was used to calculate frequency counts of the responses. Tables, graphs and charts were further constructed to illustrate the frequencies of the responses. An Impact/Probability Chart was used to analyze the probability of risk occurrences and their possible impacts on airline transportation using the Jetair Airways as a case.

4. RESULTS

The data was collected from the airline operators and IT specialists using questionnaires. This was, therefore further grouped, summarized and presented in the form of charts and tables. The questions were designed to look at security aspects such as regards to confidentiality, integrity and availability of online transactions namely, Email Address, Email Password, Phone Number, Booking Reference Number, Debit/Credit Card Number, Card Expiry Date, Card Expiry Date, Card Pin, Security Code (CVV), 3D Secure Password.

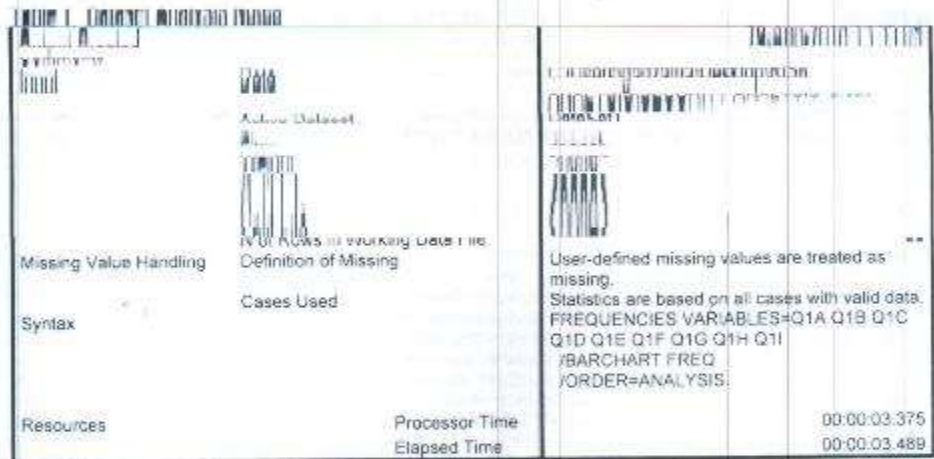


Table 2. Distribution of Questionnaires

	Email Address	Email Password	Phone Number	Booking Reference Number	Debit/Credit Card Number	Card Expiry Date	Card Pin	Security Code (CVV)	3D Secure Password
N Valid	50	50	50	50	50	50	50	50	50
Missing	0	0	0	0	0	0	0	0	0



What would happen if customers' information such as Email Address, Email Password, Phone Number, Booking Reference Number, Debit/Credit Card Number, Card Expiry Date, Card PIN, Security Code (CVV) and 3D Secure Password was made public? (Confidentiality)

Table 3. Responses on Email Address Confidentiality

	Frequency	Percent	Valid Percent	Cumulative Percent
Very Low	16	32.0	32.0	32.0
Low	10	20.0	20.0	52.0
Medium	7	14.0	14.0	66.0
High	7	14.0	14.0	80.0
Very High	10	20.0	20.0	100.0
Total	50	100.0	100.0	

Table 4. Responses on Email Password Confidentiality

	Frequency	Percent	Valid Percent	Cumulative Percent
Very Low	1	2.0	2.0	2.0
Low	3	6.0	6.0	8.0
Medium	4	8.0	8.0	16.0
High	16	32.0	32.0	48.0
Very High	26	52.0	52.0	100.0
Total	50	100.0	100.0	

Table 5. Responses on Phone Number Confidentiality

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid: Very Low	10	20.0	20.0	20.0
Low	10	20.0	20.0	40.0
Medium	10	20.0	20.0	60.0
High	13	26.0	26.0	86.0
Very High	7	14.0	14.0	100.0
Total	50	100.0	100.0	



Table 6. Responses on Booking Reference Number Confidentiality

	Frequency	Percent	Valid Percent	Cumulative Percent
Valid Very Low	5	10.0	10.0	10.0
Low	1	2.0	2.0	12.0
Medium	19	38.0	36.0	50.0
High	15	30.0	30.0	80.0
Very High	10	20.0	20.0	100.0
Total	50	100.0	100.0	

Table 7. Responses on Debit/Credit Card Number Confidentiality

	Frequency	Percent	Valid Percent	Cumulative Percent
Very Low	6	12.0	12.0	12.0
Low	3	6.0	6.0	18.0
Medium	7	14.0	14.0	32.0
High	17	34.0	34.0	66.0
Very High	17	34.0	34.0	100.0
Total	50	100.0	100.0	

Table 8. Responses on Card Expiry Date Confidentiality

	Frequency	Percent	Valid Percent	Cumulative Percent
Very Low	11	22.0	22.0	22.0
Low	17	22.0	22.0	44.0
Medium	8	16.0	16.0	60.0
High	10	20.0	20.0	80.0
Very High	10	20.0	20.0	100.0
Total	50	100.0	100.0	

Table 9. Responses on Card Pin Confidentiality

	Frequency	Percent	Valid Percent	Cumulative Percent
Very Low	1	2.0	2.0	2.0
Low	1	2.0	2.0	4.0
Medium	6	12.0	12.0	16.0
High	3	6.0	6.0	22.0
Very High	39	78.0	78.0	100.0
Total	50	100.0	100.0	

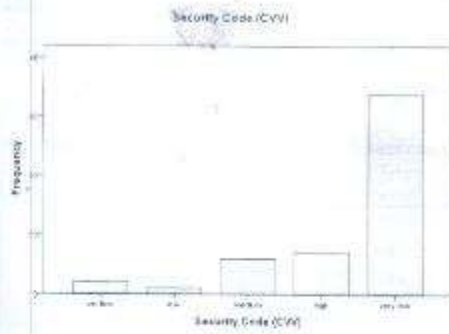


Figure 8. Responses on Email Security Code Confidentiality



Figure 9. Responses on 3D Secure Password Confidentiality

What would happen if customers' information such as Email Address, Email Password, Phone Number, Booking Reference Number, Debit/Credit Card Number, Card Expiry Date, Card PIN, Security Code (CVV) and 3D Secure Password was incorrect? (Integrity)

Table 12. Responses on Email Address Integrity

	Frequency	Percent	Valid Percent	Cumulative Percent
Very Low	14	28.0	28.0	28.0
Low	11	22.0	22.0	50.0
Medium	8	16.0	16.0	66.0
High	8	16.0	16.0	82.0
Very High	9	18.0	18.0	100.0
Total	50	100.0	100.0	

Table 13. Responses on Email Password Integrity

	Frequency	Percent	Valid Percent	Cumulative Percent
Very Low	6	12.0	12.0	12.0
Low	3	6.0	6.0	18.0
Medium	9	18.0	18.0	36.0
High	15	30.0	30.0	66.0
Very High	17	34.0	34.0	100.0
Total	50	100.0	100.0	



Table 14. Responses on Phone Number Integrity

	Frequency	Percent	Valid Percent	Cumulative Percent
Very Low	3	6.0	6.0	6.0
Low	12	24.0	24.0	30.0
Medium	16	32.0	32.0	62.0
High	10	20.0	20.0	82.0
Very High	9	18.0	18.0	100.0
Total	50	100.0	100.0	

Table 15. Responses on Booking Reference Number Integrity

	Frequency	Percent	Valid Percent	Cumulative Percent
Very Low	5	10.0	10.0	10.0
Low	2	4.0	4.0	14.0
Medium	13	26.0	26.0	40.0
High	20	40.0	40.0	80.0
Very High	10	20.0	20.0	100.0
Total	50	100.0	100.0	

Table 16. Responses on Debit/Credit Card Number Integrity

	Frequency	Percent	Valid Percent	Cumulative Percent
Very Low	6	12.0	12.0	12.0
Low	1	2.0	2.0	14.0
Medium	9	18.0	18.0	32.0
High	15	30.0	30.0	62.0
Very High	19	38.0	38.0	100.0
Total	50	100.0	100.0	

Table 17. Responses on Card Expiry Date Integrity

	Frequency	Percent	Valid Percent	Cumulative Percent
Very Low	10	20.0	20.0	20.0
Low	7	14.0	14.0	34.0
Medium	14	28.0	28.0	62.0
High	7	14.0	14.0	76.0
Very High	12	24.0	24.0	100.0
Total	50	100.0	100.0	



Table 18. Responses on Card Pin Integrity

	Frequency	Percent	Valid Percent	Cumulative Percent
Very Low	3	6.0	6.0	6.0
Low	2	4.0	4.0	10.0
Medium	2	4.0	4.0	14.0
High	13	26.0	26.0	40.0
Very High	30	60.0	60.0	100.0
Total	50	100.0	100.0	

Table 19. Responses on Security Code Integrity

	Frequency	Percent	Valid Percent	Cumulative Percent
Very Low	2	4.0	4.0	4.0
Low	2	4.0	4.0	8.0
Medium	4	8.0	8.0	16.0
High	14	28.0	28.0	44.0
Very High	28	56.0	56.0	100.0
Total	50	100.0	100.0	

Table 20. Responses on 3D Secure Password Integrity

	Frequency	Percent	Valid Percent	Cumulative Percent
Very Low	1	2.0	2.0	2.0
Low	1	8.0	8.0	10.0
Medium	4	34.0	34.0	44.0
High	17	54.0	54.0	98.0
Very High	27	2.0	2.0	100.0
Total	50	100.0	100.0	

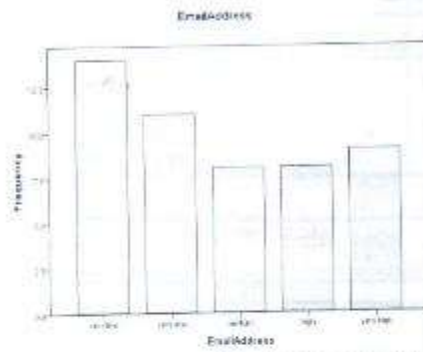


Figure 10. Responses on Email Address Integrity

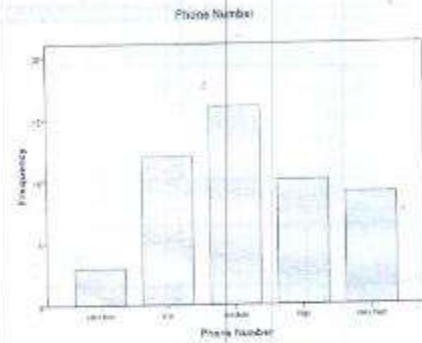


Figure 12. Responses on Phone Number Integrity

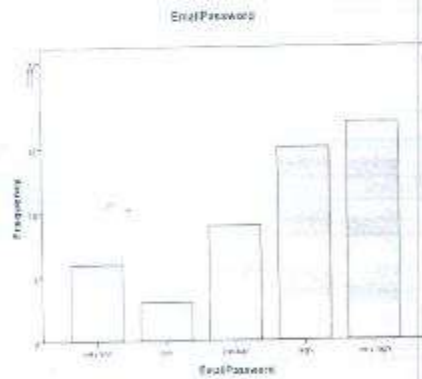


Figure 11. Responses on Email Password Integrity

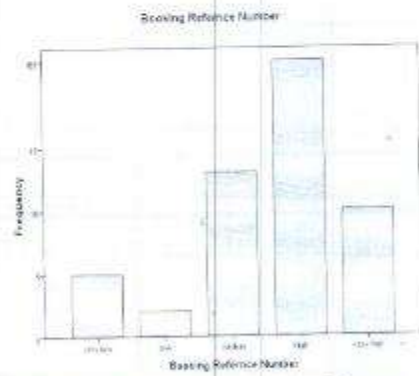


Figure 13. Responses on Booking Reference Number Integrity



What would happen if customers couldn't access their information such as Email Address, Email Password, Phone Number, Booking Reference Number, Debit/Credit Card Number, Card Expiry Date, Card PIN, Security Code (CVV) and 3D Secure Password? (Availability)

Table 21. Responses on Email Address Availability

	Frequency	Percent	Valid Percent	Cumulative Percent
Very Low	9	18.0	18.0	18.0
Low	6	12.0	12.0	30.0
Medium	14	28.0	28.0	58.0
High	7	14.0	14.0	72.0
Very High	14	28.0	28.0	100.0
Total	50	100.0	100.0	

Table 22. Responses on Email Password Availability

	Frequency	Percent	Valid Percent	Cumulative Percent
Very Low	2	4.0	4.0	4.0
Low	4	8.0	8.0	12.0
Medium	12	24.0	24.0	36.0
High	14	28.0	28.0	64.0
Very High	18	36.0	36.0	100.0
Total	50	100.0	100.0	

Table 23. Responses on Phone Number Availability

	Frequency	Percent	Valid Percent	Cumulative Percent
Very Low	4	8.0	8.0	8.0
Low	7	14.0	14.0	22.0
Medium	17	34.0	34.0	56.0
High	12	24.0	24.0	80.0
Very High	10	20.0	20.0	100.0
Total	50	100.0	100.0	

Table 24. Responses on Booking Reference Number Availability

	Frequency	Percent	Valid Percent	Cumulative Percent
Very Low	3	6.0	6.0	6.0
Low	5	10.0	10.0	16.0
Medium	17	34.0	34.0	50.0
High	17	34.0	34.0	84.0
Very High	8	16.0	16.0	100.0
Total	50	100.0	100.0	

Table 25. Responses on Debit/Credit Card Number Availability

	Frequency	Percent	Valid Percent	Cumulative Percent
Very Low	3	6.0	6.0	6.0
Low	9	18.0	18.0	24.0
Medium	8	12.0	12.0	36.0
High	20	40.0	40.0	76.0
Very High	12	24.0	24.0	100.0
Total	50	100.0	100.0	

Table 26. Responses on Card Expiry Date Availability

	Frequency	Percent	Valid Percent	Cumulative Percent
Very Low	6	12.0	12.0	12.0
Low	13	26.0	26.0	38.0
Medium	5	10.0	10.0	48.0
High	15	30.0	30.0	78.0
Very High	11	22.0	22.0	100.0
Total	50	100.0	100.0	

Table 27. Responses on Card Pin Availability

	Frequency	Percent	Valid Percent	Cumulative Percent
Very Low	4	8.0	8.0	8.0
Low	4	8.0	8.0	16.0
Medium	11	22.0	22.0	38.0
High	31	62.0	62.0	100.0
Total	50	100.0	100.0	



Table 28. Responses on Security Code Availability

	Frequency	Percent	Valid Percent	Cumulative Percent
Very Low	2	4.0	4.0	4.0
Low	3	6.0	6.0	10.0
Medium	14	28.0	28.0	38.0
High	9	18.0	18.0	56.0
Very High	22	44.0	44.0	100.0
Total	50	100.0	100.0	

Table 29. Responses on 3D Secure Password Availability

	Frequency	Percent	Valid Percent	Cumulative Percent
Very Low	1	2.0	2.0	2.0
Low	4	8.0	8.0	10.0
Medium	6	12.0	12.0	22.0
High	14	28.0	28.0	50.0
Very High	25	50.0	50.0	100.0
Total	50	100.0	100.0	

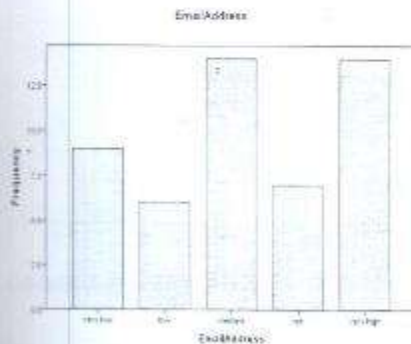


Figure 19. Responses on Email Address Availability

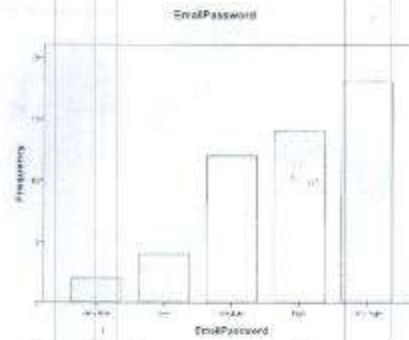


Figure 20. Responses on Email Password Availability

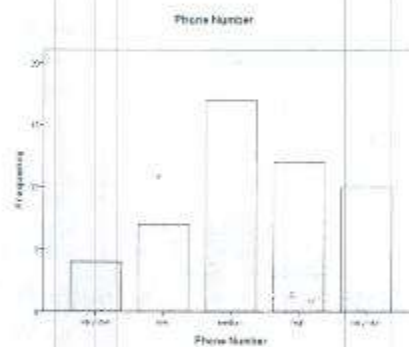


Figure 21. Responses on Phone Number Availability

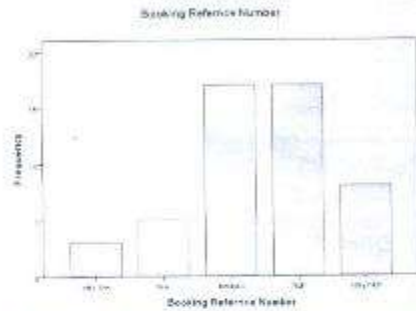


Figure 22. Responses on Booking Reference Number Availability

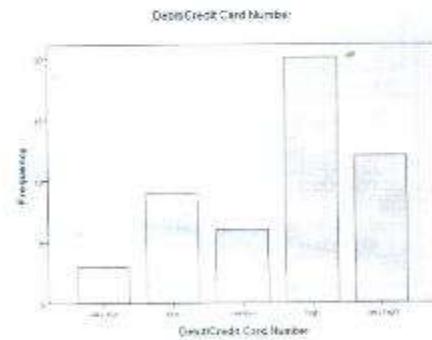


Figure 23. Responses on Debit/Credit Card Number Availability

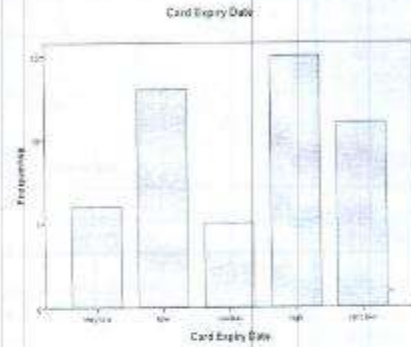


Figure 24. Responses on Card Expiry Date Availability

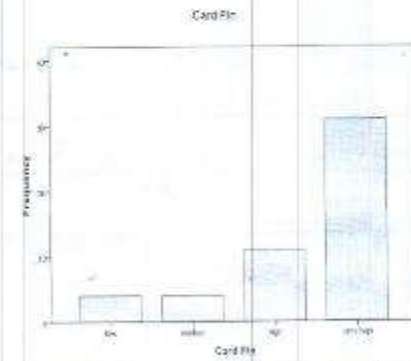


Figure 25. Responses on Card Pin Availability

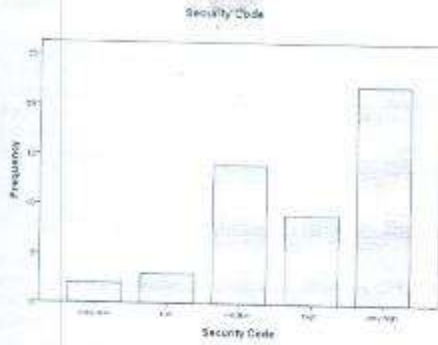


Figure 26: Responses on Security Code Availability

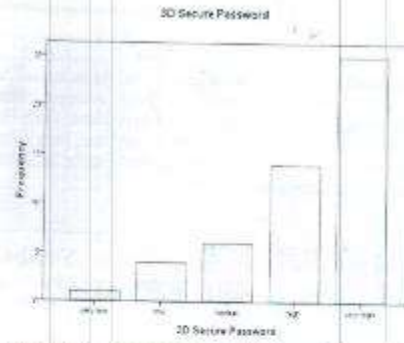


Figure 27: Responses on 3D Secure Password Availability

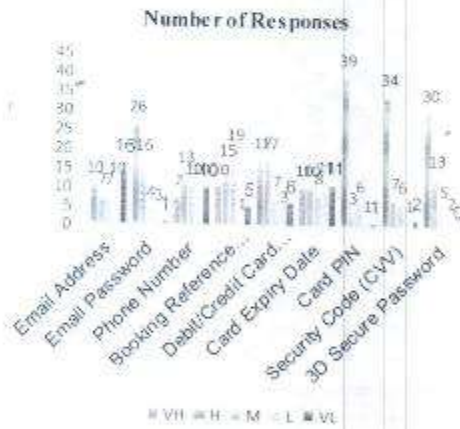


Figure 28: Overall Responses on Confidentiality



In the study conducted, respondents were asked to express their views on what they think would happen if customers' information such as Email Address, Email Password, Phone Number, Booking Reference Number, Debit/Credit Card Number, Card Expiry Date, Card PIN, Security Code (CVV) and 3D Secure Password was made public. Five options were provided namely; Very High (5 points), High (4 points), Medium (3 points), Low (2 points) and Very Low (1 point). Table 30 and Figure 28 establish that the Pin Number has the highest rating of the overall score for confidentiality with 39.

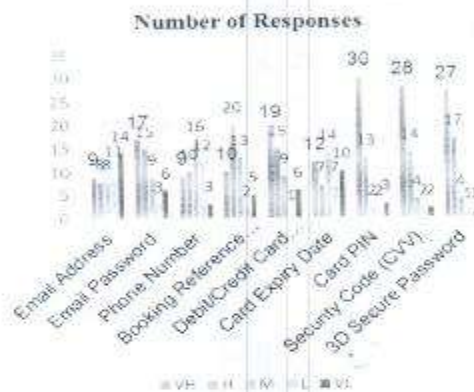


Figure 29. Overall Responses on Integrity

Table 30: Overall Responses on Confidentiality

	VH	H	M	L	VL
Email Address	9	8	8	11	14
Email Password	17	15	9	3	6
Phone Number	9	10	16	12	3
Booking Reference Number	10	20	13	2	5
Debit/Credit Card Number	19	15	9	1	6
Card Expiry Date	12	7	14	7	10
Card PIN	30	13	2	2	3
Security Code (CVV)	28	14	4	2	2
3D Secure Password	27	17	4	1	1



Table 31. Overall Responses on Integrity

	VH	H	M	L	VL
Email Address	14	7	14	6	9
Email Password	18	14	12	4	2
Phone Number	10	12	17	7	4
Booking Reference Number	8	17	17	5	3
Debit/Credit Card Number	12	20	6	9	3
Card Expiry Date	11	15	5	13	6
Card PIN	31	11	4	4	0
Security Code (CVV)	22	9	14	3	2
3D Secure Password	25	14	6	4	1

In response to what would happen if customers' information such as Email Address, Email Password, Phone Number, Booking Reference Number, Debit/Credit Card Number, Card Expiry Date, Card PIN, Security Code (CVV) and 3D Secure Password was incorrect, Table 31 and Figure 29 show that Pin Number has the highest rating of the overall score with 30.

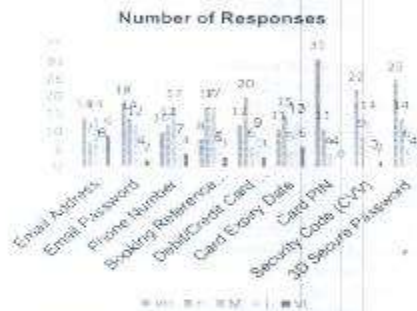


Figure 30. Overall Responses on Availability

Regarding what would happen if customers couldn't access their information such as Email Address, Email Password, Phone Number, Booking Reference Number, Debit/Credit Card Number, Card Expiry Date, Card PIN, Security Code (CVV) and 3D Secure Password, Table 32 and Figure 30 indicate that Pin Number has the highest rating of the overall score for integrity with 31.

Table 32. Overall Responses on Availability

	VH	H	M	L	VL
Email Address	14	7	14	6	9
Email Password	18	14	12	4	2
Phone Number	10	12	17	7	4
Booking Reference Number	8	17	17	5	3
Debit/Credit Card Number	12	20	6	9	3
Card Expiry Date	11	15	5	13	6
Card PIN	31	11	4	4	0
Security Code (CVV)	22	9	14	3	2
3D Secure Password	25	14	6	4	1



5. DISCUSSION

The discussion section examines the results of data collected during the study, in relation to research questions. The questions posed in the first section of this paper were discussed and answered separately. The fundamental purpose of the study was to analyse security risk analysis and management of Jumia Air Travel.

With the increasing dependence of people on Internet and ICT, the existing literature has shown that it is important for organisations to protect their information assets against cyber threats to avoid IT security occurrences.

Panda et al. (2006) indicated that all segments of society had become more dependent upon networking and IT, and this same technology became an increasingly tempting target for malicious activity. Graham et al. (2011) also observed that every day, new vulnerabilities and malicious code threatened systems on networks. Maskun et al. (2013) specified three (3) classes of attacks that were possible from Internet, namely service disruption, theft of assets, as well as capture and control. They advised further that to eliminate or dismiss cyber risks, protection of cyberspace infrastructure is needed in order to stop hackers from committing crimes.

In agreement with the aforementioned authors, it would be equally important that the Jumia Air Travel implement cyber security best practices to prevent or reduce cyber risks. Furthermore this implementation of cyber security best practices would be required to maintain the confidentiality, integrity and availability of information. Barman (2002) advised that the only way to understand your infrastructure was to perform a full risk analysis on the entire enterprise and then ensured that information security policies appropriately addressed diverse threats.

What would happen if customers' data such as Email Address, Email Password, Phone Number, Booking Reference Number, Debit/Credit Card Number, Card Expiry Date, Card PIN, Security Code (CVV) and 3D Secure Password was made public, incorrect and inaccessible?

Data was believed to be the main target of attack to information systems. The study considered the protection of data at rest, in processing as well as data in transit via communication channels. There is need for data to be protected against unauthorized access and integrity violation. From Tables 30, 31, 32 and Figures 28, 29, 30, it would be established that the Pin Number has the highest rating of the overall scores.

The implication of the result is that Jumia Air Travel should ensure that the highest-rated information (Pin Number) needed to be more protected than other information with a low ratings. Also, there is the need to develop and implement appropriate measures to maintain plans for resilience and to restore any capabilities or services that may be impaired due to a security risk incident. Other important aspects viewed to be crucial in the management of security risks include: configuration management and control, business continuity and disaster recovery, incident response planning, security training, physical / logical security, personnel security, security assessments, access control mechanisms and encryption technologies.

What strategies can be employed to mitigate risks facing the Jumia Air Travel?

Based on the risks identified, the study encouraged that appropriate security measures should be in place to ensure that information assets remain secured and that whatever might happen should not lead to a complete disaster that might halt the Jumia Air Travel operations. To determine the appropriate strategies that needed to be employed by Jumia Air Travel there was a need to carry out an assessment of risks identified during the study. This was also supported by Rok and Borka (2008) when they stated that once security risks have been identified, they must be assessed as to their potential loss and to the probability of occurrence. They defined this assessment as the determination of potential effect of an individual risk by assessing the likelihood and impact should it occur. Thus, to successfully address cyber security risks in the Jumia Air Travel, the attention and resources should go to the very high and high priority areas through adopting various suitable strategies.

The Risk Mitigation Strategy

Mitigation is the choice of reducing the impact of the resulting damage to an acceptable level. The mitigation strategies are required to minimize the magnitude or impacts of the residual risks. It is important that the Jumia Air Travel identifies appropriate mitigation strategies for the various risks identified during the study. The Jumia Air Travel is required to perform a cost-benefit analysis and decide on the best possible strategies based on the risks at hand. The mitigation strategy options are as explained below.



Risk Acceptance: is a strategy that is taken when the cost of other management options such as avoidance or limitation is greater than the cost of the risk itself.

Risk Avoidance: this is the action that avoids any exposure to the risk. Avoidance is the choice to avoid a risk by removing the source and/or consequences. For instance, deleting some functions in the system or even removing the whole system. The Jumia Air Travel needed to look at obsolete systems that could no longer be updated, old operating systems and applications that are no longer supported by their developers and perform security risk analysis.

Risk Limitation: is the act of trying to minimize the impact of the risk. Limitation is the choice to mitigate the impact of vulnerability exploitation by implementing proper information security systems or tools such as antivirus or firewall or implementing proper security policies such as access control or passwords.

Risk Transference: Involves handing over the risk to a third party if it cannot be handled internally. Transference is the choice to shift risk to other assets, processes or organizations by outsourcing information security services, buying rethinking how services are offered, revising deployment models or implementing service contract with providers. Therefore risks that were identified but could not be managed within the public service should be transferred to trusted service providers.

6. CONCLUSIONS

The aim of the risk assessment process is to evaluate hazards, then remove that hazard or minimize the level of its risk by adding control measures, as necessary. By this, you have created a safer and healthier workplace. To understand the risk nature of the airline industry is important in effectively managing the business. The goal of a firm is to maximize its return for the firm and its investors. The maximum return can be obtained when high-expected return coheres with low risk. Currently, there is lack of cyber security best practices in the Jumia Air Travel. This situation has made it difficult for the Organisation to analyse and manage its security risks. The study examined security risk analysis and management of Jumia Air Travel. It was established that the Pin Number had the highest rating of the overall score for confidentiality, integrity and availability. Based on the risks identified, the study encouraged that appropriate security measures should be in place to ensure that information assets remain secured and that whatever might happen should not lead to a complete disaster that might halt the Jumia Air Travel operations.

7. RECOMMENDATION

The objective of this study is to minimize the security risks facing online information assets of the Jumia Air Travel and decide on appropriate strategies to mitigate the resulting dangers. To enable the Jumia Air Travel meet the desired stage, the following recommendations were made:

- Development of organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
- Development and implementation of appropriate activities to identify the occurrence of a cybersecurity event.
- Staff members should be educated on the secure and unsecure online practices.
- They should be educated on the importance of maintaining foundational security measures.
- Development of topic specific policies including e-mail policies, password policies, and internet policies is necessary.
- Make cyber security training a compulsory requirement for all employees and educate them how security can benefit their daily works.

Acknowledgments

Support for this work was provided by the management and staff of Nnamdi Azikiwe International Airport Abuja and Khemsale Computers Academy Kaduna. I would like to thank respondents for their input, I would also like to thank the management of Jumia Air Travel as well as my colleagues who provided immense support and important feedback. I am highly indebted to Dr Samuel A. Ojeniyi and Dr Olawale O. Adebayo of the Department of Cyber Security Federal University of Technology Minna who offered useful suggestions and painstakingly reviewed this Work. I deeply appreciate the kind patience of my wife and children throughout the period of writing this paper.



REFERENCES

- [1] An, M., Noh, Y., 2009. Airline customer satisfaction and loyalty: impact of in-service quality. *Serv. Bus.* 3 (3), 293-307
- [2] Barman, S. (2002) Writing information security policies. New York: New Riders
- [3] Bernstein, P. (1996). *Against the Gods: The Remarkable Story of Risk*. Chichester: Wiley
- [4] Canadian Air Transport Security Authority Act Review Secretariat (2006). *Flight Plan: Managing the Risks in Aviation Security*. Report of the Canadian Air Transport Security Act Review Advisory Panel, Ottawa.
- [5] Chen, F.Y., Chang, Y.H., 2005. Examining airline service quality from a process perspective. *J. Air Transp. Manag.* 11, 79-87
- [6] Cox, A., & Townsend, M. (1998). *Strategic Procurement in Construction*. London, UK: Thomas Telford.
- [7] Crawford, M., Stein, W. 2002. Auditing risk management: fine in theory but who can do it in practice? *International Journal of Auditing* 6, 119-131.
- [8] Curry, N., Gao, Y., 2012. Low-cost airlines - a new customer relationship? An analysis service satisfaction, and customer loyalty in a low-cost vice: measuring the gap. *J. Serv. Res.* 9 (9), 109 - 138
- [9] Fone, M., & Young, P. (2000). *Public Sector Risk Management*. London, UK: Butterworth-Heinemann
- [10] Hood, J., & Young, P. (2005). Risk financing in UK local authorities: is there a case for risk pooling? *International Journal of Public Sector Management*, 18(6), 563-76.
- [11] Lintner, J. (1965). Security prices, risk and maximal gains from diversification. *Journal of Finance*, 20(4), 587-615
- [12] March, J. G., & Shapira, Z. (1987). Managerial perspectives on risk and risk taking. *Management Science*, 33(11), 1404-18
- [13] Maskun, & Manuputy, A., & Noor S.M. & Sumardi J. (2013). Cyber Security: Rule Of Use Internet Safety? 13th *International Educational Technology Conference, Procedia - Social and Behavioral Sciences* 103, 255 - 261
- [14] Moore, P. G. (1983). *The Business of Risk*. Cambridge, UK: Cambridge University Press.
- [15] Panda, B., Giordano, J., & Kail, D. (2006). Next-Generation: Cyber Forensics. *Communications of the ACM*, 49(2), 44-47.
- [16] Park, J.W., Robertson, R., Wu, C.L., 2004. The effect of airline service quality on Taiwan. *J. Am. Acad. Bus. Camb.* 9 (2), 324-330
- [17] Rhoades, D.L., Waguespack Jr., B., 2008. Twenty years of service quality performance stores. *Serv. Quali.* 18 (1), 20-33
- [18] Robledo, M.A., 2001. Measuring and managing service quality: integrating customer expectations. *Manag. Serv. Qual.* 11 (1), 22-31
- [19] Rok, B., & Borika, J. (2008). An economic modelling approach to information security risk management. *International Journal of Information Management* 28, 413-422
- [20] Saha, G.C., Theingi, 2009. Service quality, satisfaction, and behavioural intentions. *Manag. Serv. Qual. An Int. J.* 19 (3), 350 -372
- [21] Sharpe, W. F. (1963). A simplified model of portfolio analysis. *Management Science*, 9(2), 425-442.
- [22] Sheel, A. (1995). An empirical analysis of anomalies in the relationship between earnings' yield and returns of common stock: The case of hotel and lodging firms. *The Council on Hotel, Restaurant and Institutional Education*, 18(3), 13-24.
- [23] Smallman, C. (1996). Risk and organisational behaviour: a research model. *Disaster Prevention and Management*, 5(2), 12-26.
- [24] Thomson, M.E., O' nkal, D., Avcolu, A., Goodwin, P., 2004. Aviation risk perception: a comparison between experts and novices. *Risk Analysis* 24, 1585-1595.
- [25] Tsaur, S.H., Chang, T.Y., Yen, C.H., 2002. The evaluation of airline service quality by. *Manag.* 23 (2), 107-115
- [26] Webb, J., Ahmad, A., Sean B. Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers & Security* 44, 115



FEDERAL UNIVERSITY OF TECHNOLOGY MINNA
SCHOOL OF INFORMATION AND COMMUNICATION TECHNOLOGY
DEPARTMENT OF CYBER SECURITY SCIENCE

QUESTIONNAIRE ON SECURITY RISK ANALYSIS AND MANAGEMENT IN AIRLINE TRANSPORTATION
USING JUMIA AIR TRAVEL AS A CASE STUDY

Dear Respondent,

This questionnaire is designed to provide information on Security Risk Analysis and Management in Airline Transportation using Jumia Air Travel as a Case Study. The information gathered would be strictly used for researched purpose. You are kindly requested to be objective and respond to every item sincerely based on your personal opinions. Information given will be treated with utmost confidentiality.

Thank you for your anticipated cooperation.

Yours sincerely,

GADZAMA Emmanuel Hamman
(Researcher)

SECTION A

Demographic Data of Correspondents used for the Study.

Name:

Gender: Male Female

Organisation:

Department/Section:

Specialty:

Others:



SECTION B

Instruction: Kindly tick (✓) the appropriate option of the questionnaire to indicate your opinion.

Key: Very High (5); High (4); Medium (3); Low (2); Very Low (1)

1. What would happen if these data are disclosed to any unauthorized individual? (Confidentiality)	5	4	3	2	1
Email Address					
Email Password					
Phone Number					
Booking Reference Number					
Debit/Credit Card Number					
Card Expiry Date					
Card PIN					
Security Code (CVV)					
3D Secure Password					
2. What would happen to if these information are incorrect? (Integrity)	5	4	3	2	1
Email Address					
Email Password					
Phone Number					
Booking Reference Number					
Debit/Credit Card Number					
Card Expiry Date					
Card PIN					
Security Code (CVV)					
3D Secure Password					
3. What would happen if one couldn't access these information? (Availability)	5	4	3	2	1
Email Address					
Email Password					
Phone Number					
Booking Reference Number					
Debit/Credit Card Number					
Card Expiry Date					
Card PIN					
Security Code (CVV)					
3D Secure Password					