"Were We Ready in the First Place?": An Analysis of Cashless Policy Implementation in Nigeria

Oluwafemi Osho
+2348034106811

Temidayo H.Ajisola
+2347063194947

Agada D. Onoja
+2347039165474

Joel N. Ugwu
+2348063305810

ABSTRACT

On 1st January, 2012, Nigeria commenced the implementation of cashless policy, with the kick-off in Lagos State. By the end of that year it was evident the implementation could not be extended to other states of the federation, as earlier scheduled. This raised a crucial question: was Nigeria prepared in the first place, in terms of availability of needed infrastructures, to commence implementation of the cashless economy? This study seeks to answer this question. In addition, it identifies potential consequences of implementation on the security of the nation's cyberspace. Both primary and secondary data were collected. Our findings reveal that when the implementation of the cashless policy kicked-off, awareness, required infrastructures, and the security of the country's cyberspace were inadequate. We suggest that the consequences of implementing cashless policy in Nigeria will have various security effects on the Nigerian cyberspace if the level of awareness and existing infrastructures are not improved.

CCS Concepts

• **Information systems →Information systems application →Web applications →Electronic commerce →Secured online transactions**

Keywords

Cashless society, cashless economy, cashless policy, implementation, subscribe.

1. INTRODUCTION

A cashless economy is one in which a given society is regulated to have the least needed amount of cash in circulation, the rest of which is transacted electronically through the use of direct debit, mobile payments, electronic fund transfer, internet banking, multi-functional Automated Teller Machines (ATMs), point of sale terminals (POSs), amongst others [1], [2]. Simply put, a cashless economy entails a pervasive application of various computer technologies in the financial system [3]. The system gives way for goods and services to be purchased by individuals without anything tangible being exchanged, using what is known as electronic cash. The term money still exists, but it is more in an electronic processes form than previously.

An effective and modernized payment system has been found to be positively correlated with the development of the economy [4], [5], being a tool for more effective, convenient and faster methods of buying goods and rendering of services. This explains why several governments and their financial institutions have been taking steady steps towards achieving a cashless society.

The benefits of adoption of cashless economy include reduction in corruption and the cost of services by banks (such as cost of credit), increased operational efficiency, improved financial inclusion, via providing alternatives that aid easy transactions and greater reach, and improved efficiency of the monetary policy in managing the rate of inflation and driving the growth of the economy [4], [6], [7], [8], [9]. Other benefits include increased convenience in transaction; promotion of e-commerce; reduction in circulation of fake currency, theft of cash from individuals, money laundering, and stockpiling of cash in houses by corrupt government officials [6], [8], [10].

However, implementing cashless policy poses some risks. Since personal information and data will now reside online, it becomes increasingly difficult to curb internet hackers and thieves. Other demerits are potential increase in cyber crimes, increased sophistication in operation of hackers and scammers, increase in theft of ATM, credit and debit cards, to mention but few [4], [8], [11]. This underscores why a secure national cyberspace is fundamental to the success of cashless policy implementation.

Activities of hackers and other cyber criminals have always posed different threats to the cyberspace. Activities such as phishing attack, website spoofing by masquerading, creating different entity similar to the operated entity, identity theft, virus attacks, key loggers and cracking encryption channels that are guarding a system are capable of stifling the capacity of the cyberspace to support effective implementation of the cashless policy. As a result of these, the need for necessary facilities to ensure effectiveness, efficiency, security, privacy, integrity, confidentiality, convenience, acceptability, mobility, for successful actualization of cashless economy cannot be overemphasized.

In line with the nation's vision 20:20, which is being among the first 20 economies by year 2020 [8], to enable the development and modernization of the payment system, to attain reduction in cost of banking services, improve financial inclusion and effectiveness of monetary policy, the cashless policy was introduced in Nigeria, with a test run in Lagos in 1st January, 2012 [4], [5]. On 6th January 2013, the Central bank of Nigeria (CBN) suspended the spread of the cashless policy from Lagos state to other states. Some of the contributing factors included insufficient POS, ATM, and low level of awareness, connectivity, and bandwidth penetration. Other challenges included low ICT penetration and other logistics issues [12]. The suspension raised some pertinent issues: was Nigeria prepared in the first place to commence implementation of the cashless economy? And having

CoRI'16, Sept 7–9, 2016, Ibadan, Nigeria.

commenced, what are the potential consequences on the security of the nation's cyberspace.

This study seeks to assess the level of readiness of Nigeria, in respect of provisioning of required infrastructures, when the implementation of the policy commenced in 2012, and identify possible implications of implementation considering the current state of her cyberspace. This study is significant in many ways. First, it would expose the state of Nigeria's cyberspace at the commencement of implementing cashless policy. It also assesses the current capacity of the cyberspace to effectively support the policy. These would provide decision makers, including the government, relevant agencies, IT managers, policy makers, and other stakeholders, responsible for the Nigerian cashless policy implementation, better insight into the security implications, which would enable them to implement necessary strategies towards more effective implementation.

2. LITERATURE REVIEW

2.1 Requirements for Effective Implementation of Cashless Policy

Effective implementation of cashes policy is predicated on the availability of some requirements. These are divided into hardware, software, legal, personnel, and logistic requirements.

2.1.1 Hardware Requirement

Some of the hardware requirements include computer systems; smart (debit and credit) cards, used as alternative to cash for making purchases, for making withdrawals or deposits at ATMs, updating account information and for other transactions made in the banks. Others are smart phones, which provide services such as multimedia message service (MMS), email, short-range wireless communications (infrared and bluetooth), text messaging, internet access, business applications, supporting online transactions [9], [13], [14]; and Point-of-Sale (POS) terminals [6], an **e**quivalent of an electronic cash register, which aids transactions through the use of smart chip cards, credit cards, debit cards, and other electronically-dependent transactions in a traditional retail environment.

2.1.2 Software Requirement

These are the software components used to drive and secure the different hardware. They include phishing detection tools, to detect and block suspicious sites. For example, when a customer transacts on a fake website, these tools can be used to detect the Domain Name System (DNS) roots of the sites. Anti-phishing software can be installed on the customer's computer, so as to detect addresses that are not on the database during a transaction. Another requirement is antivirus software. They are used in detecting, preventing and removing malware such as virus, worms, hijacker, key loggers, root kits, Trojan horses, spyware, and backdoors. Antivirus software enhances computer security, protecting it from social engineering attacks. Real time protection and access scanning are provided by most antivirus, anti-spyware and anti-malware software. It prevents attackers from having access to banking information [14]. A third requirement in this category is firewall. This filters information coming into a computer system or private network through the internet, preventing flagged packet of information from going through. Firewalls are used in controlling traffic flowing in and out of the network. They can be used to prevent direct connection between bank-end systems and to address security concerns of external deceives such as ATMs and PCs that are in connection to the bank's network. They protect computers from remote login, application backdoors, Simple Mail Transfer Protocol (SMTP) session hijacking and macros. One other important software requirement is intrusion detection system (IDS). This is a software application or hardware device that monitors network systems for policy violations and malicious activities. Identifying possible incidents, logging information and reporting attempts are primarily the functions of IDS. The IDS can be either host-based or network-based [15].

2.1.3 Legal Requirement

The legal requirement consists of relevant laws, standards, policies, and regulations to clearly define the roles and regulate the activities of the different stakeholders in the system. An important component is the development of relevant policies on cyber security. These based on national leadership, sharing of responsibilities, partnership with all concerned agencies, active international engagement, risk management control. They enhance both collective and individual security. According to [16], the objectives of these policies are to the effect that all citizens should be adequately aware of cyber risks and how their computers can be secure, thereby protecting their finances, online privacy and identities; to ensure smooth operations and privacy of customers; and for the government to ensure security of the country's information and communications technologies and make them resistant to attack from malicious hackers.

Also pertinent for effective implementation of cashless policy are cyber laws. The availability, confidentiality, and integrity of information being stored, processed, and communicated electronically is ultimate. Therefore, relative measures have to be taken to this regard. As there might be an ill effect from an increase in cybercrime on the economy, country and society at large, there is need for activities of law enforcement, regulatory detection, and strong legal frameworks to enhance the operations of a cashless economy. Strong legislative Acts are required for comprehensive, effective and unified legal framework catering for the prevention, detection, banning, prosecution, and punishment for cyber crimes in the nation [14].

A third component is the monetary policy. Cashless policy enhances the payment system of a country. It regulates the cash collection and lodgment in the country and stipulates that there exists a monitor and feedback mechanism that allows the full adoption and smooth implementation of cashless economy in a country. A monetary policy ensures that there is a limit to cash withdrawal and lodgment fees for corporate and individual customers [14], [17].

2.1.4 Personnel Requirement

These comprise Payment Terminal Services Provider (PSTP), Computer Emergency Response Team (CERT), Communications and Media Authority (CMA), and the Attorney-General's Department (AGD). PTSPs, amongst other things, are engaged in proper maintenance/support of infrastructure to ensure effectiveness of POS operations. Their services include all aspects relating to both terminal management and support, and not limited to purchase and replacement of spare parts, provision of training, repairs, connectivity, and development of value-added services [14]. The CERT facilitates information sharing and improves response co-ordination to cyber threats between citizens and the Government. They help in identifying and analyzing high level cyber-attacks as well as other cyber events, aiding response across the private sector systems and government infrastructure. They ensure that access to information on cyber security threats are available to the community, including vulnerabilities in their systems, how information can be better protected and the potential consequences of an incidence in the information technology environment [16].

The Communications and Media Authority (CMA) is responsible for broadcasting regulations on the internet, radio and telecommunications. It contributes to the objectives of cyber security by gathering evidence, assisting in preventing identity theft, computer fraud and regulatory obligations in regard to criminal misuse and illegal act, and makes sure standards are met by the telecommunications providers and Internet Service Providers (ISPs). The last component of this requirement, the Attorney-General's Department (AGD), consists of security policy protection departments, criminal law and the law enforcement that collectively provide harmonization of cyber security policies, which includes international collaboration and crisis management as well as protection of security policies for government agencies. They oversee such government business partnerships as CERT, and provide guidance on cyber security to owners and critical infrastructure operators [16].

2.1.5 Logistics Requirement

The logistic requirement includes standards on application and system software; standards for computer network and internet; and high speed/broadband internet technologies, which describes a broad range of technologies that provides higher rate of data access to the internet, supporting faster World Wide Web (WWW) browsing, file download, virtual private networks and remote system administration [14]. Also, there is absolute need for international engagement. The global challenges of cyber security require multilateral or bilateral efforts with key ally nations to strengthen cyberspace. Increase in multilateral forums with relevant international bodies is necessary to enhance international efforts in development of global standards, legal system capacity to combat cybercrime, promotion of situational awareness, strategic warning and even response [16].

2.2 Implementing Cashless Policy in Nigeria

Prior to the commencement of the implementation of the cashless policy in Nigeria, the banking sector was rife with investment environments characterized by high risk, corruption, payment fraud, poor credit administration, lack of credit facility, and system unreliability [4]. Having identified the need to reduce significantly the industry's cost to serve, the CBN, in alliance with the Banker's committee, initiated a shared service program with five key areas in focus: cash management, payment systems transformation, IT infrastructure and services, IT standards, and back office operations. Transformation of the payments system became the key driver. Out of the payments transformation initiative was borne the cashless policy [18]. The policy was aimed, amongst many, to reduce cost of maintenance of cash-based economy by 90% [19].

Part of the efforts by the CBN towards modernizing the payments system was initiating the National Payments System (NPS) in 2005 [5], automating the cheque clearing system through the introduction of an MICR-based technology and the first automated clearing process in Lagos [4]. Other efforts include establishment of frameworks and guidelines on payments system [4], licensing of Payments Terminal Service Providers (PTSPs) and 14 mobile payment schemes, campaigns and public awareness [18]. Banks and non-bank stakeholders also embarked on measures to promote the cashless initiative. Within the space of seven months, the number of PoS terminals increased from 6,019 to 89,700 [7]; number of registered merchants reached 151,717 by July 2012 [5]. Major initiatives in the implementation of the cashless policy are presented in Figure 1 [20].

After wide consultations with relevant stakeholders, the implementation of the policy, termed 'Cashless Lagos,' kicked off in Lagos on 1st January, 2012 [4], [18] and was expected to commence officially in the rest of the country by January, 2013 [5], [8]. Seven months into the implementation of the policy in Lagos, many challenges had surfaced: insufficient and unevenly spread PoS terminals, many instances of deployed but yet-to-be-configured PoS terminals, frequent network downtime which were affecting completion of transactions, Short Cash conversion cycle, lack of clarity on allocation of handling charges, transparency in the manner settlements were to be carried out for PoS transactions, clearly-defined data and network security standards across electronic payment channels, and availability and stability of mobile money platforms [7]. Nweke [5] recommended some pre-conditions that should be met before the proposed nationwide take-off in 2013. These, amongst others, included provision of necessary payment infrastructure: power supply, mobile telecoms infrastructure, electronic clearing technology; relevant legal and regulatory framework, and a law enforcement agency equipped to adequately tackle cyber-crime and internet fraud. However, overwhelmed by the challenges during the 'Cashless Lagos' exercise, the earlier plan to extend the cashless policy to the rest of the country was readjusted to commence in the Federal Capital Territory (Abuja), Abia, Anambra, Kano, Ogun, and River States effective July 1, 2013.

A critical appraisal reveals that the introduction of the cashless policy has recorded little success [21]. In spite of measures so far deployed, e-payment fraud has continued to pervade the country's banking-sphere. In six months, up to ₦20 billion was lost to fraudsters. This was despite report by CBN on reduction in ATM card fraud upon the introduction of chip-and-PIN cards [21], and institution of ATM Anti-Fraud Committee, which was upscaled to E-Payment Fraud Forum [18]. There were instances where hackers were found to fix tools on ATMs that harvest passwords of customers who come to transact using the machines. In 2013 alone, according to CBN, ₦40 billion was lost to electronic frauds [22].

3. MATERIALS AND METHODS

To achieve our objectives of assessing the level of readiness of Nigeria, in respect of provisioning of required infrastructures, when the implementation of the policy was commenced in 2012, and identifying possible implications of implementation considering the current state of her cyberspace, the study used both primary and secondary data. We believe effective implementation is anchored on adequate awareness and availability of necessary infrastructures. Consequently, we collected self-report data to collate views on the state of these factors. Also, relevant documents are investigated to ascertain the available quantity and/or quality, as the case may be, of selected basic requirements, during the period when the implementation of the cashless policy was commenced in Nigeria. The variables are then compared with international standards and/or world average. The indices are used to determine the adequacy or otherwise of the requirements. Specifically, in respect of infrastructures, the study focused on the e-index of the country; number of available ATMs, POSs; availability of broadband technology, enabling laws, CERT; and the authentication methods commonly in use.

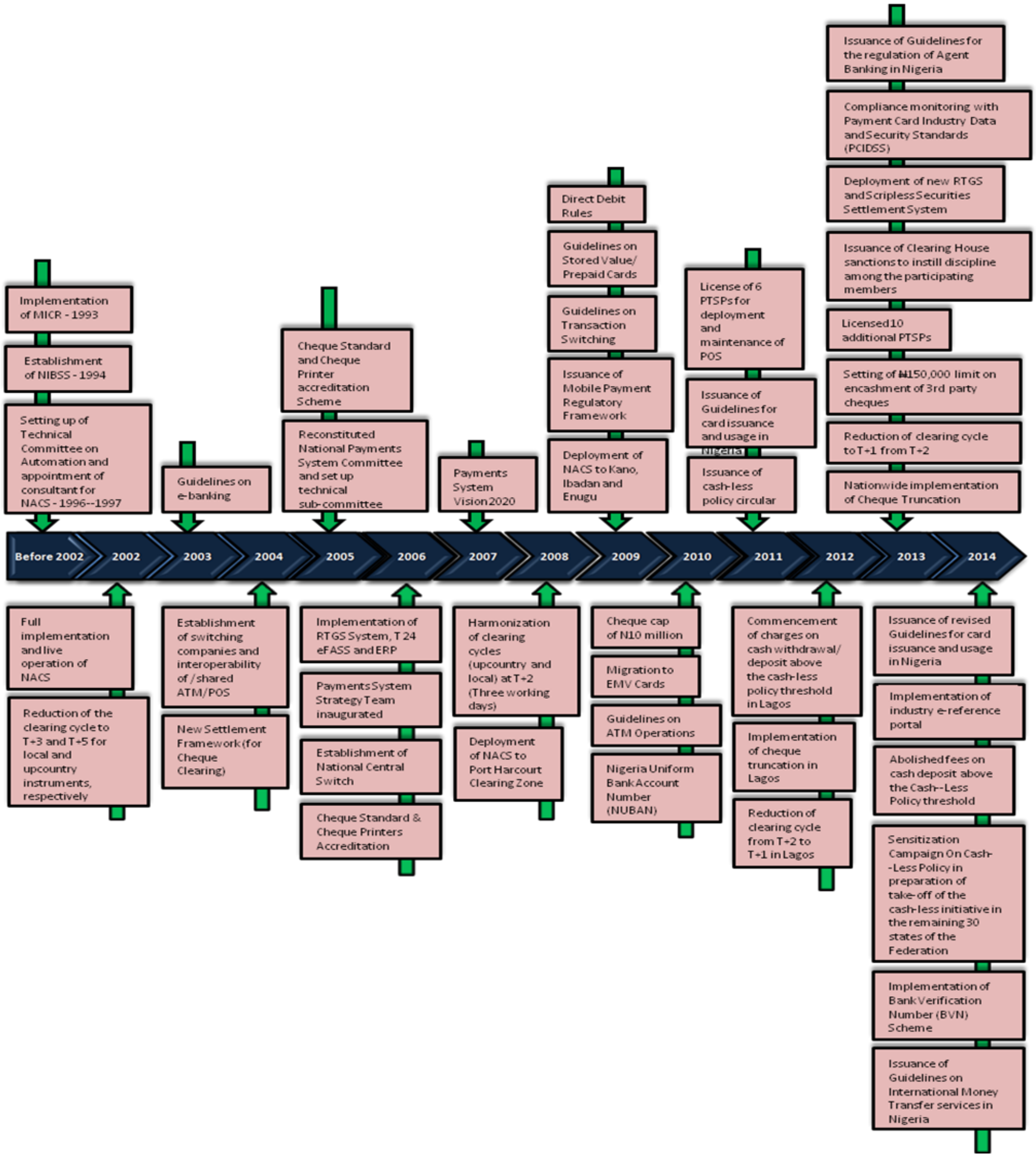
Implementation of MICR - 1993
Establishment of NIBSS - 1994
Setting up of Technical Committee on Automation and appointment of consultant for NACS - 1996--1997
Guidelines on e-banking
Cheque Standard and Cheque Printer accreditation Scheme
Reconstituted National Payments System Committee and set up technical sub-committee
Payments System Vision 2020
Direct Debit Rules
Guidelines on Stored Value/ Prepaid Cards
Guidelines on Transaction Switching
Issuance of Mobile Payment Regulatory Framework
Deployment of NACS to Kano, Ibadan and Enugu
License of 6 PTSPs for deployment and maintenance of POS
Issuance of Guidelines for card issuance and usage in Nigeria
Issuance of cash-less policy circular
Issuance of Guidelines for the regulation of Agent Banking in Nigeria
Compliance monitoring with Payment Card Industry Data and Security Standards (PCIDSS)
Deployment of new RTGS and Scripless Securities Settlement System
Issuance of Clearing House sanctions to instill discipline among the participating members
Licensed 10 additional PTSPs
Setting of ₦150,000 limit on encashment of 3rd party cheques
Reduction of clearing cycle to T+1 from T+2
Nationwide implementation of Cheque Truncation
Before 2002
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
Full implementation and live operation of NACS
Reduction of the clearing cycle to T+3 and T+5 for local and upcountry instruments, respectively
Establishment of switching companies and interoperability of / shared ATM/POS
New Settlement Framework (for Cheque Clearing)
Implementation of RTGS System, T 24 eFASS and ERP
Payments System Strategy Team inaugurated
Establishment of National Central Switch
Cheque Standard & Cheque Printers Accreditation
Harmonization of clearing cycles (upcountry and local) at T+2 (Three working days)
Deployment of NACS to Port Harcourt Clearing Zone
Cheque cap of N10 million
Migration to EMV Cards
Guidelines on ATM Operations
Nigeria Uniform Bank Account Number (NUBAN)
Commencement of charges on cash withdrawal/ deposit above the cash-less policy threshold in Lagos
Implementation of cheque truncation in Lagos
Reduction of clearing cycle from T+2 to T+1 in Lagos
Issuance of revised Guidelines for card issuance and usage in Nigeria
Implementation of industry e-reference portal
Abolished fees on cash deposit above the Cash--Less Policy threshold
Sensitization Campaign On Cash--Less Policy in preparation of take-off of the cash-less initiative in the remaining 30 states of the Federation
Implementation of Bank Verification Number (BVN) Scheme
Issuance of Guidelines on International Money Transfer services in Nigeria

Figure 1. Some major milestones in the implementation of the cashless policy [20]

3.1 Participants

To collate primary data, a survey was conducted in 2013 in Lagos, Ekiti, and Niger States. The choice of Lagos was natural being the state where the cashless policy implementation was kicked off. The research instrument used was questionnaire. A total of 250 questionnaires were distributed. Out of these, 219 were returned. 37 were found to be invalid. Consequently, 182 were used for analysis. There were slightly more male respondents, 51.6% v. 48.4%. Most were within the ages of 21 – 30 (46.7%), students (56.0%), and aware of the term cashless society and government's plan to implement it (87.9%). The demographic compositions of the respondents are presented in Table 1.

Table 1. Demographic profile of respondents

		Freq	%
Sex			
	Male	94	51.6
	Female	88	48.4
	Total	182	100.0
Age			
	< 20	42	23.1
	21 – 30	85	46.7
	31 – 40	35	19.2
	41 – 50	16	8.8
	51 – 60	3	1.6
	> 60	1	0.5
	Total	182	100.0
Occupation			
	Student	102	56.0
	Employed	61	33.5
	Unemployed	19	10.4
	Total	182	100.0
Aware of the term cashless society and government's plan to implementate it			
	Yes	160	87.9
	No	22	12.1
	Total	182	100.0

3.2 Measures

The questionnaire used for the survey had three sections. The first section sought information on respondent demographics. The second section bordered on perception about government's effort in terms of awareness, the country's readiness in respect of availability of necessary facilities, and the security of the nation's cyberspace to support implementation of the cashless policy. In the last section, respondents were asked if they were willing to subscribe to the cashless policy, considering the state of infrastructures. Those who expressed unwillingness were then requested to select reason(s). Respondents were also asked to indicate potential consequences of implementation, considering the state of infrastructures. Lastly, they were asked if they would be willing to subscribe if necessary requirements are put in place.

4. FINDINGS

4.1 Readiness to Implement Cashless Policy

As can be seen from Table 2, most respondents believed the government did not do enough, in terms of creating awareness of the cashless policy (84.6%), and necessary infrastructures were not adequately put in place (89.6%) before the implementation of the policy was commenced in 2012. Equally, most felt the country's cyberspace was not secure enough to support the kick-off of the implementation (87.9%).

Respondents who were unemployed, compared with those who were students and employed, were most critical of the government in their failure to adequately create awareness of the policy. Specifically, 94.7% of unemployed, 90.2% of students, and 72.1% of employed respondents reported government effort was insufficient. The study was found to be significant ($\chi^2(1) = 11.238,\ p = 0.004$).

In terms of adequacy of infrastructures provided for the kick-off of the cashless policy, more of the females, compared to the male, 96.6% v. 83.0%, felt the available infrastructures were inadequate ($\chi^2(1) = 9.007,\ p = 0.003$). In the same vein, more females, 97.7% v. 78.7%, rated the country's cyberspace not secure enough to support implementation of the policy ($\chi^2(1) = 15.446,\ p < 0.001$).

Table 2. Assessment of readiness to implement cashless policy

		Freq	%
Adequacy of awareness by government			
	Yes	28	15.4
	No	154	84.6
	Total	182	100.0
Adequacy of necessary facilities			
	Yes	19	10.4
	No	163	89.6
	Total	182	100.0
Security of the country's cyberspace			
	Yes	22	12.1
	No	160	87.9
	Total	182	100.0

4.1.1 E-Index

The ICT Development Index (IDI) is a composite index which is used to combine 11 indicators into one benchmark measure (presented on a scale from 0 to 10) that compares and monitors the developments in information and communication technology (ICT) across countries. A country with Low level of ICT development, indicated by an IDI value below or equal to 2.33, is not making enough effort into catching up in terms of ICT developmental progress. This group of countries, referred to as least connected countries (LCCs), has very low levels of ICT uptake and use. Between 2011 and 2012, these countries recorded the smallest increase in the average IDI value. In majority of LCCs, internet access are very limited, low-speed, very expensive and used by small percentage of the population. LCCs also tend to have very low fixed and mobile broadband penetration levels, and most only launched and commercialized 3G mobile-broadband networks relatively. The LCCs include many of the world's least developed countries (LDCs), with majority in Africa. They also include some highly populated countries that are not LDCs, such as Nigeria, India and Pakistan. Considering the ICT Development Index (IDI) for 2011 and 2012, Nigeria was ranked 123 in 2011 and 122 in 2012 out of 157 countries in the world [23].

4.1.2 PoS Terminals

As at March, 2012 the PoS density per 100,000 people in Nigeria was 13. Countries such as India had 67 PoS per 100,000 adults, Kenya had 88, Namibia 338, Uganda 453, , Malaysia and South Africa 1,063, Singapore 1,889, United State 2156, Brazil 2193, New Zealand 3,916, and Australia 3,939 [5],[18], [24].

4.1.3 ATM

In 2012, the value for ATMs per 100,000 adults in Nigeria was only 11.9, while other country such as Thailand had 77.95, South Africa 60.01, Brazil 120.6, United Kingdom 122.77, United State 173.43, Australia 166, Canada 208.98, and Japan 129.04 [24].

4.1.4 Availability of Broadband Technology

In the area of broadband, while 2G mobile enjoyed significant coverage, which was at 98%, 3G technology coverage was less than 35%. And this was found to be mostly focused in the urban areas. Though, internet penetration had attained 33%, broadband penetration was only at a mere 6% [25].

4.1.5 Enabling Laws

By 2012, necessary bills such as Cyber Security Bill and Cybercrime Bill were yet to be passed by the Nigerian National Assembly. Even the likes of Information Protection Agency Bill, Computer Security and Critical Information Infrastructure Protection Bill, the Cyber Security and Data Protection Agency bill, the Electronic Fraud Prohibition Bill, Computer Misuse Bill were all pending in the National House of Assembly, yet to become law [26].

4.1.6 Authentication Methods in Use

The authentication mechanism used by banks for transactions in Nigeria was mainly log-in passwords. However, in addition to the password, some of the banks also adopted the use of hardware token and PINs [27].

4.1.7 Availability of CERT

As at 2012, when the implementation of cashless policy was commenced, Nigeria had no CERT to share information, identify, analyze sophisticated cyber attacks and respond to cyber security threat.

4.2 Willingness to Subscribe to Cashless Policy and Potential Consequences of Implementation

When asked to indicate their intention to subscribe to the cashless policy, considering the state of infrastructures which they had agreed were inadequate, slightly more respondents (52.7%) indicated they were willing. Compared to the employed and unemployed, the students were most willing in subscribing to the policy, regardless of the state of the infrastructures. The percentage among students, employed, and unemployed respondents were 63.7%, 42.6%, and 26.3% respectively. The finding was significant ($\chi^2(1) = 12.766,\ p =\ 0.002$). Having understanding about the concept of cashless economy and knowledge of government's decision to implement it was found to increase the likelihood of subscribing to the policy. While 55.6% of those aware of what cashless economy was were willing to subscribe, only 31.8% of those who reported they had no understanding indicated willingness. This finding was equally significant ($\chi^2(1) = 4.398,\ p =\ 0.036$).

Among those who were unwilling to subscribe, low awareness level ranked as the most common reason (77.9%). Other reasons indicated by most in this category were potential increase in card theft (61.6%), fear of leakage of sensitive personal information (55.8%), and unavailability/insufficiency of required infrastructures (53.5%).

For potential consequences of commencing the implementation of the cashless policy, considering the state of infrastructure, most of the respondents believed it would lead to increase in card theft (77.5%), number of hackers (72.0%), internet or cybercrimes (68.1%), and sophistication of hackers' operations (60.4%).

When requested again to indicate their willingness to subscribe to the policy, with necessary infrastructures in place, 94.5% of the respondents reported they would subscribe.

Table 3. Willingness to subscribe to cashless policy and potential consequences of implementation

	Freq	%
Willingness to subscribe, considering state of infrastructures		
Yes	96	52.7
No	86	47.3
Total	182	100.0
Reason(s) for unwillingness to subscribe		
Low awareness level	67	77.9
Unavailable/insufficient infrastructures	46	53.5
Inefficient operators	40	46.5
Likely increase in card theft	53	61.6
Fear of leakage of sensitive personal information	48	55.8
Nigerian government cannot be trusted	40	46.5
Others	11	12.8
Potential consequences of implementation of cashless policy		
Increase in card theft	141	77.5
Increase in internet or cybercrimes	124	68.1
Increase in number of hackers	131	72.0
Increased sophistication in operations of hackers	110	60.4
Increased privacy risk of customers' information	84	46.2
Others	13	7.1
Willingness to subscribe if necessary requirements are put in place		
Yes	172	94.5
No	10	5.5
Total	182	100.0

5. DISCUSSION

The objective of this study was evaluating how ready Nigeria was, in the provisioning of necessary requirements, when the implementation of the policy commenced in 2012, and identifying potential implications of implementation considering the current state of her cyberspace. From the findings, most respondents were aware of concept of cashless economy and government's plan to implement it. Confirming the results of [4], [7], [28], the level of awareness by relevant bodies was inadequate. In the same vein, most respondents believed availability of necessary infrastructures, and the security of the country's cyberspace were inadequate at the time implementation of cashless policy was commenced in Nigeria in 2012. Secondary data supported these findings.

A critical look at the current level of implementation makes evident the fact that most of the challenges, which were cyber-related, are still being faced. For instance, the CBN set a target for the deployment of over 400,000 PoS terminals in 2015, with the hope of accelerating PoS density in the country to 2,247 per

100,000 people by the end of the same year [18], [29]. However, by first half of 2014, number of deployed PoS was 121,886 [30]. By 2015, the number was still around this range [31]. In 2014, number of ATMs had increased to just 16.05 per 100,000 adults [32]. In 2014, fixed broadband penetration was 0.01 per 100 people, international internet bandwidth was 3.15 bits/sec per internet user, and by 2015, the number of secure internet servers was 3 per million people [33]. These could have been responsible for the poor connectivity experienced by PoS users in Lagos, as reported by [28] as part of their findings.

Respondents who were willing to subscribe to the cashless policy despite inadequate infrastructures were slightly more than those not interested. However, with necessary infrastructures in place, almost all were willing. The study revealed that the willingness to subscribe was influenced by some demographic characteristics. Though almost all the students agreed that the government did not do enough in terms of creating awareness, they were most willing to subscribe to the policy when it was commenced. One possible explanation of this finding is the perceived performance expectancy on subscribing to the policy. This entails the extent to which a subscriber believes the policy would help achieve some gains in job performance. Age has been found to moderate this variable, with the effect stronger for younger subscribers [34]. Relatively, students fall under this category.

Those who knew what cashless economy was about, and also knew about government's plan to implement it were also found to be more willing to subscribe. This underscores the necessity of adequate awareness. Not surprisingly, inadequate awareness was found to be the biggest factor that influenced apathy towards the cashless policy. Other factors cited by those unwilling to subscribe centered on online security risks and inadequate infrastructures.

5.1 Implications, Limitations, and Further Studies

It is evident, from our study, that Nigeria was not well prepared, considering the level of awareness and available infrastructures, when the implementation of the cashless policy commenced in 2012. This submission corroborates part of the findings of [6]. Consequently, we suggest that the implications of implementing cashless policy in Nigeria will have various security effects on the Nigerian cyberspace, if proper requirements are not put in place. Specifically, if the states of infrastructures are not upgraded, most respondents reported likely increase in card theft, number of hackers, internet or cybercrimes, and sophistication of hackers' operations. These findings agree with those of [6] and [11], as cited by [19].

Our study is not without some limitations. Using self-report data always poses the problem of generalization. For instance, the findings might have been different if the entire data were collected in Lagos alone. Additionally, the number of alternatives available for those who were unwilling to subscribe to and as potential consequences of implementation of the policy was not exhaustive. Future studies could explore a more exhaustive list of options. No doubt, new challenges must have been identified since the commencement of the policy.

6. CONCLUSION

From our study, it was evident that Nigeria was ill-prepared when the implementation of cashless policy was kicked-off in Lagos in 2012. Unfortunately, much has not changed in terms of available infrastructures. This poses potential risks to the cyberspace, and much more the economy, of the country. These findings highlight the necessity of continuous and more intense awareness, increasing and improving existing infrastructures, and strengthening the security of the cyberspace.

7. REFERENCES

[1] Ezuwore-Obodoekwe, C. N., Eyisi, A. S., Emengini, S. E., & Chukwubuzo, A. F. 2014. A critical analysis of cashless banking policy in Nigeria. *IOSR J Bus Manag*, 16, 5 (May. 2014), 30-42.

[2] Okoye, P. V.C. and Ezejiofor, R. 2013. An Appraisal of Cashless Economy Policy in Development of Nigerian Economy. *Research Journal of Finance and Accounting.* 4, 7, 237-252.

[3] Oluwabiyi, A. A. 2015. Policy Implications of Cashless Banking on Nigeria's Economy. *Public Policy and Administration Research.* 5, 3, 214-220.

[4] Atanda, A. A., and Alimi, O. Y. 2012. Anatomy of Cashless Banking in Nigeria. *Centre for Management, Development & Policy Modelling (CMDPM)*, 1-20.

[5] Nweke, F. 2012. *Nigeria in 2012: The Vision of Cash-less Economy*. Delivered at the J-K Gadzama & Partners LLP 2012 Annual Public Lecture.

[6] Akhalumeh, P. B., and Friday, O. 2012. Nigeria's Cashless Economy: The Imperatives. *International Journal of Management and Business Studies*, 2, 2, 31-36.

[7] Lamikanra, B. 2012. Managing the transition to a cashless economy in Nigeria: The Challenges and Strategies. *Presentation at the Nigeria Computer Society (NCS) 24th National Conference* (July, 2012).

[8] Ovat, O. O. 2012. The Central Bank of Nigeria's Cashless Policy in Nigeria: Benefits and Challenges. *Journal of Economics and Sustainable Development,* 3, 14, 128-133.

[9] Sunday, O. 2013. Facing the home truth of cashless policy, *IT & Telecom digest*. Retrieved January 25, 2013 from http//www.ittelecomdigestcom.

[10] Ochei, L. C. 2012. Effective Strategies for Monitoring and Controlling Overspending in a Cashless Society: Lessons for Citizenship Empowerment. *African journal of computing & ICT*, 5, 5, 159-162.

[11] Akhalumeh, P. B and Ohiokha, F. 2012. Nigeria's Cashless Economy: The Imperatives. *International journal of management & business studies,* 2, 12, 31-36.

[12] Akanbi, F. 2013. *Cashless Policy: Shift in Take-off Dates in Order, Say CBN, Experts*. Thisday Live (2013, January 6). Retrieved from http://www.thisdaylive.com/articles/cashless-policy-shift-in-take-off-date-in-states-in-order-say-cbn-experts/135481/

[13] Akinola, O.S., 2012. Cashless Society, Problems and Prospects, Data Mining Research Potentials. *International Journal of Computer Science and Telecommunications*, 3, 8, 49-55.

[14] CBN, 2003. *Guidelines on Electronic Banking in Nigeria*. Retrieved May 14, 2013 from http://www.nibss-plc.com.ng/wp-content/uploads/2012/07/E-BANKING.pdf

[15] Wu, T. M. 2009. *Intrusion detection system* (6thed) Information Assurance Technology Analysis Center (IATAC).Woodland park, Herndon.

[16] Robert, M. 2009. *Cyber Security strategy, Australian government*. Retrieved June 16, 2013 from http://www.ag.gov.au/cybersecurity

[17] BFA, 2013. *What does the CBN's Cash-less policy mean for financial inclusion in Nigeria?* Bankable Frontier Associate. Retrieved February 10, 2013 from http://www.efina.org.ng/assets/manualUploads/EFInAWhat-does-the-CBNs-Cash-less-policy-mean-for-financial-inclusion-in-NigeriaMarch-2013.pdf

[18] Lemo, T. 2012. Lessons from Nigeria's Cashless Society Campaign. *Keynote presentation at the AITEC Banking and Mobile Money Conference (*March, 2012).

[19] Muyiwa, O., Tunmibi, S., and John-Dewole, A. T. 2013. Impact of Cashless Economy in Nigeria**.** *Greener Journal of Internet, Information and Communication Systems*, 1, 2, 040-043.

[20] CBNa. *Payments System – Introduction.* Retrieved July 9, 2016 from https://www.cbn.gov.ng/Paymentsystem/

[21] Nweze, C. 2015. *Electronic banking: Little gains, more pains*. The Nation Newspaper (May 11, 2015). Retrieved May 11, 2015 from http://thenationonlineng.net/new/electronicbankinglittle-gainsmorepains/

[22] Abioye, O. 2015. *Hackers hit bank ATMs in Lagos*. The Punch Newspaper (April 7, 2015). Retrieved April 7, 2015 from http://www.punchng.com/business/business-economy/hackershitbankatmsinlagos/

[23] ITU, 2013. *Measuring Information Society*. Retrieved February 5, 2014 from http://www.itu.int/go/mis2013

[24] World Bank, 2013. *World development indicator: financial access, stability and efficiency*. Retrieved from http://wdi.worldbank.org/table/5.5

[25] Presidential Committee on Broadband. *Nigeria's National Broadband Plan 2013 – 2018*. Retrieved July 8, 2016 from http://www.researchictafrica.net/countries/nigeria/Nigeria_National_Broadband_Plan_2013-2018.pdf

[26] Osho, O., Falaye A. A., and Shafi'I, M. A. 2013. Combating Terrorism with Cyber security: the Nigerian perspective. *World journal of computer application and technology,* 1, 4. 103-109.

[27] Lawal, O. B. Ibitola, A. Longe, O .B. 2013. Internet Banking Authentication Methods in Nigeria Commercial Banks. *African Journal of computer & ICT,* 6, 1, 208-215.

[28] NIBSS. 2015. *PoS Adoption and Usage: A Study on Lagos State.* Retrieved July 8, 2016 http://www.nibss-plc.com.ng/wp-content/uploads/2015/05/NIBSS-2015-POS-Adoption-Study-Lagos-State.pdf

[29] CBN, 2011. *Guidelines on Point of Sale (POS) Card Acceptance Services*. Retrieved from http://www.cbn.gov.ng/cashless/POS_GUIDELINES_August2011_FINAL_FINAL%20(2).pdf

[30] CBNb. *Payments System – Payment Modes in Nigeria.* Retrieved July 9, 2016 from https://www.cbn.gov.ng/Paymentsystem/Modes.asp

[31] News Agency. 2015. *CBN: Nigerians make N1.5bn transactions on POS daily.* The Cable (Oct. 7, 2015). Retrieved July 9, 2016 from https://www.thecable.ng/cbn-nigerians-make-n1-5bn-transactions-pos-daily

[32] World Bank. 2016a. *World Development Indicators: Financial access, stability and efficiency*. Retrieved June 30, 2016 from http://wdi.worldbank.org/table/5.5#

[33] World Bank. 2016b. *World Development Indicators: The Information society*. Retrieved June 30, 2016 from http://wdi.worldbank.org/table/5.12#

[34] Venkatesh, V., Morris, M. G., Davis, G. B., and Davis, F. D. 2003. User acceptance of information technology: Toward a unified view. *MIS quarterly* (Sept. 2003), 27, 3, 425-478.