MALETE JOURNAL OF ACCOUNTING AND FINANCE
A Publication of the Department of Accounting and Finance, Faculty of Management and Social Sciences, Kwara State University, Malete
Vol. 4 No. 2, June, 2024 ISSN: 2735-9603

EFFECT OF E-GOVERNANCE POLICY ON SECURITY IN NIGERIA

[1]Bashi B Musa, [2]Abu Idris, [3]Yusuf Abdulhakeem and [4]Ndagi Salihu

[1,2 &4]Ibrahim Badamasi Babangida University, Lapai, Niger State, Nigeria
[3]Federal University Dursin-Ma, Katsina State-Nigeria
[1]donbashsilver@yahoo.com
[2]idrisa@ibbu.edu.ng
[3]ayusuf21@fudutsinma.edu.ng

Abstract
Security is a fundamental pillar for the stability and development of societies worldwide. E-Governance policy, which involves the use of digital tools and technologies in government operations, has emerged as a critical strategy for addressing modern security challenges. This study investigates the effect of E-Governance policy on security in Nigeria. The sample was drawn from 806 personnel of the Police Intelligence Department (FID), comprising the Intelligence Response Team (IRT) and Special Tactical Squad (STS) located at the force headquarters in FCT, Abuja. Multiple regression analysis and descriptive statistics were employed to achieve the study's objectives. The major findings reveal that digital incidence reporting systems (DIRS) have a significant positive relationship with security; digital forensic tools (DFT) have a significant positive relationship with security; and CCTV surveillance systems have a significant positive relationship with security. The study concludes that if the Nigerian government focuses on providing digital incidence reporting systems, digital forensic tools, and CCTV surveillance systems, it will lead to an improved security situation in the country. It is recommended that the government at all levels allocate sufficient resources for the procurement, maintenance, and upgrade of these digital tools and systems. Additionally, the study recommends that the Nigerian government partner with international organizations and experts to provide specialized training and certification programs for Nigerian security personnel. Furthermore, the government should establish continuous monitoring and evaluation mechanisms to assess the performance and impact of digital incidence reporting systems, digital forensic tools, and CCTV surveillance.

Keywords: Security; e-governance; digital incidence, reporting systems; forensic tools

INTRODUCTION

Security is a fundamental pillar for the stability and development of societies worldwide. It has been widely argued that insecurity and violent extremism negatively impact economic growth in the short run through various channels (Yusuf & Mohammad, 2023). In the 21st century, the nature of security threats has evolved, encompassing not only traditional concerns like crime and terrorism but also digital and cyber threats. According to the United Nations Office on Drugs and Crime (2019), the global homicide rate was 6.1 per 100,000 people in 2019, highlighting the persistent challenge of violent crime across various regions. Additionally, the rise of cybercrime has become a significant concern, with global damages estimated to reach $6 trillion annually by 2021. These statistics underscore the urgent need for innovative technological solutions to enhance

security frameworks globally.

E-Governance, which involves the use of digital tools and technologies in government operations, has emerged as a critical strategy in addressing modern security challenges. By leveraging technology, governments can enhance transparency, efficiency, and responsiveness in managing public safety and security (Yusuf & Mohammad, 2023). Key e-Governance tools such as digital incidence reporting systems, digital forensic tools, and CCTV surveillance systems play crucial roles in contemporary security management. These tools facilitate real-time data collection, analysis, and dissemination, thereby improving the ability of law enforcement agencies to prevent, detects, and responds to criminal activities effectively.

In Africa, the adoption of (electronic governance) e-Governance tools has been gaining momentum as countries seek to enhance their security apparatus amidst rising crime rates and security challenges. The African Union has recognized the potential of digital solutions in its Agenda 2063, which emphasizes the need for modernized security frameworks. For instance, South Africa has implemented advanced CCTV systems in major cities like Johannesburg and Cape Town, resulting in notable reductions in certain types of crime (African Union, 2019). In Kenya, digital forensic tools have been instrumental in solving complex criminal cases, demonstrating the effectiveness of these technologies in the African Union (African Union, 2019).

Nigeria, Africa's most populous country, faces significant security challenges, including terrorism, armed robbery, kidnapping, and cybercrime. According to the Nigerian National Bureau of Statistics (2020), the country recorded over 1,500 kidnapping incidents in 2020, highlighting a severe security concern. The Nigerian government's response includes adopting e-Governance tools to bolster its security framework. The risk and uncertainty associated with rising levels of insecurity cause Foreign Direct Investments (FDI) to be redirected away from countries with higher security risks toward those with lower risks. Increased levels of insecurity reduce investment returns, thereby diminishing foreign direct and portfolio investments in developing countries (Chuku et al., 2019). Rising levels of insecurity and anti-national activities pose significant challenges to national rules and regulations, human rights, and have a considerable negative impact on the economy. These issues affect various economic and social parameters, including prices, output, employment, trade balance, poverty, inequality, defense expenditure, government budget patterns, and the socio-political environment (Isola et al., 2019).

The motivation for Nigeria's adoption of e-Governance tools in addressing security issues is multifaceted. Firstly, the integration of technology enhances the efficiency and effectiveness of security operations, ensuring timely and accurate responses to incidents. Secondly, it promotes transparency and accountability within security agencies, reducing the incidence of corruption and misuse of power. Lastly, e-Governance tools facilitate better resource management and strategic planning, enabling data-driven decisions that improve overall security outcomes (IFAC, 2024). Until recently, studies on the drivers of e-governance in Nigeria were predominantly conceptual and lacked thorough empirical investigation. Notable studies, such as those by Jones and Smith (2021), Alshaikh et al. (2024), Smith and Anderson (2024), Vrbnjak et al. (2024), and Kossakowski and Szuba (2024), have highlighted the importance of e-governance but have not provided extensive quantitative analysis. This lack of comprehensive empirical research makes it challenging to draw scientific conclusions about the impact of e-governance policies. This study

aims to address this gap by examining the effects of e-governance policies on security in Nigeria using a quantitative approach. By doing so, it seeks to gain insights into the effectiveness of these policies and identify areas for improvement.

Research questions

This study provides answers to the following questions:

i. Does the use of Digital Incidence Reporting Systems affect security in Nigeria?
ii. Does the use of Digital Forensic Tools affect security in Nigeria?
iii. Does the use of CCTV Surveillance Systems affect security in Nigeria?

Research objectives

The general objective of the study is to investigate the impact of e-Governance policy on security in Nigeria, while the specific objectives are to:

i. Evaluate the effect of Digital Incidence Reporting Systems on security in Nigeria.
ii. Examine the effect of Digital Forensic Tools on security in Nigeria.
iii. Assess the effect of CCTV Surveillance Systems on security in Nigeria.

Research Hypotheses

Following the review of empirical investigations, the following hypotheses are formulated and tested:

H_{01}: Use of Digital Incidence Reporting Systems has no significant effect on security in Nigeria.
H_{02}: Use of Digital Forensic Tools has no significant effect on security in Nigeria.
H_{03}: Use of CCTV Surveillance Systems has no significant effect on security in Nigeria.

LITERATURE REVIEW

Security

Buzan (1991) defines security as a condition in which states and individuals have the capacity to manage threats to their survival and well-being. Buzan emphasizes that security is not limited to military threats but includes political, economic, societal, and environmental dimensions. He argues that security should be understood as freedom from fear and freedom from want, extending beyond the mere absence of conflict. Baldwin (1997) defines security in a broad context, suggesting that security should be viewed as a situation where an actor, typically a state, can protect its values from external threats. Baldwin emphasizes the subjective nature of security, noting that different actors may perceive different threats and therefore have different security needs. Waltz (1979) defines security in terms of state survival within the anarchic international system. For Waltz, security is fundamentally about maintaining sovereignty and territorial integrity against external military threats. Wolfers (1952) describe security as the absence of threats to acquired values. He highlights the dual aspects of security—objective measures (the absence of danger) and subjective feelings (the absence of fear).

e-Governance Policy

Meier (2015) defines e-governance policy as a strategic framework that employs digital technologies to enhance the protection of citizens. This includes systems for early warning, crisis communication, and the efficient mobilization of resources during emergencies to minimize harm and ensure public safety. Chen et al (2015) describes E-governance policy in relation to the security of lives encompasses the strategies and measures implemented by governments to utilize ICT for

enhancing public safety, improving emergency response capabilities, and ensuring effective communication and coordination during crises to protect citizens' lives. Nunamaker et al (2012) opined that electronic governance policy aimed at the security of lives refers to the comprehensive policies and technological solutions designed to safeguard the population through improved disaster management, real-time information dissemination, and enhanced coordination of emergency services.

Digital Incidence Reporting Systems (DIRS***)***

According to Gupta (2018), Digital Incidence Reporting Systems (DIRS) refer to technologically advanced platforms that allow for the systematic documentation, management, and analysis of incidents within an organization. These systems aim to improve safety, compliance, and operational efficiency by providing real-time reporting and data analytics. In another vein, Jones and Leonard (2020), defined DIRS as the integrated digital platforms designed to capture and manage incident reports electronically. They enhance the reporting process by ensuring accuracy, timeliness, and accessibility of incident data, thereby supporting effective incident management and decision-making. Lastly, United Nations (2021) describes Digital Incidence Reporting Systems (DIRS) as an electronic system developed to facilitate the reporting and tracking of incidents, including safety, security, and operational disruptions. These systems are essential for improving incident response times, data accuracy, and overall organizational resilience.

Digital Forensic Tools (DFT***)***

Carrier (2005) refers DFT as software applications or hardware devices specifically designed for the extraction, preservation, analysis, and presentation of digital evidence. They enable forensic investigators to uncover hidden, deleted, or encrypted data from digital storage devices. Kruse and Heiser (2002) define Digital forensic tools as a range of technologies used to systematically collect and examine digital evidence. These tools help investigators to maintain the chain of custody and ensure that the evidence is admissible in court. According to Garfinkel (2010), Digital forensic tools refer to the array of software and hardware solutions employed by forensic examiners to conduct investigations involving digital evidence. These tools support activities such as data recovery, media analysis, and the generation of forensic reports.

Closed-circuit Television (CCTV***) Surveillance Systems***

Norris and Armstrong (1999), opined that, CCTV surveillance systems consist of video cameras placed in specific locations, connected to monitors or recording devices to observe and record activities. These systems are primarily used for crime prevention, traffic monitoring, and enhancing security in public and private spaces. Welsh and Farrington (2009), defines CCTV surveillance systems as an integrated setups of cameras and recording technologies that are used to capture, store, and sometimes analyze video footage. These systems aim to deter criminal activities, assist in the identification of offenders, and provide evidence for law enforcement purposes. Gill and Spriggs (2005)describes CCTV surveillance system as a network of cameras that transmit signals to specific monitors or recording devices for the purposes of security and monitoring. The main goals of these systems include crime prevention, public safety enhancement, and evidence collection.

Theoretical Framework

This research adopts the Technology Acceptance Model (TAM)and the Institutional Theory as the

underpinning theories for this study.

Technology Acceptance Model (TAM)

Propounded by Fred D. Davis in 1989, TAM is a well-established framework that explains how users come to accept and use a technology. The Technology Acceptance Model (TAM) is a theoretical framework developed to understand and predict how users accept and use new technology. It suggests that the perceived usefulness and perceived ease of use of a system are key determinants of its acceptance and usage. The TAM has been widely used in the field of information systems to study technology adoption and usage behavior. When we relate the TAM to the topic of the effect of e-Governance policy on security in Nigeria, we can consider how the acceptance of e-Governance systems by stakeholders such as government officials, citizens, and businesses can impact the overall security landscape of the country.

Perceived Usefulness: If stakeholders perceive e-Governance systems as useful in improving transparency, efficiency, and service delivery in government operations, they are more likely to accept and use these systems. Increased use of e-Governance platforms can lead to better data management, streamlined processes, and improved decision-making in government agencies, which can ultimately enhance security measures.

Perceived Ease of Use: The ease of use of e-Governance systems, including user-friendly interfaces, accessibility, and training programs, can influence how effectively stakeholders interact with these platforms. If users find e-Governance systems easy to use, they are more likely to adopt them, leading to increased participation in digital government services and potentially enhancing security practices through better data protection and access control.

Security Concerns: One critical aspect of e-Governance policy in Nigeria is ensuring the security and privacy of data transmitted and stored on government platforms. Users' perceptions of the security measures implemented in e-Governance systems can significantly impact their acceptance and trust in these systems. A robust security framework, including encryption, authentication mechanisms, and data protection protocols, is essential to mitigate cyber threats and safeguard sensitive information in e-Governance initiatives.

Institutional Theory

John W. Meyer and Brian Rowan in their 1977 paper Institutional Theory focuses on the deeper and more resilient aspects of social structure. It considers the processes by which structures, including schemes, rules, norms, and routines, become established as authoritative guidelines for social behavior. This theory is essential for understanding the regulatory, normative, and cognitive aspects of e-Governance implementation in Nigeria:

Regulatory Pillar: Examines how laws and regulations around e-Governance policies affect security protocols and enforcement.

Normative Pillar: Looks at the roles of professional and social norms in shaping the acceptance and effectiveness of e-Governance for security purposes.

Cognitive Pillar: Investigates how shared understandings and beliefs about e-Governance influence its adoption and integration into existing security frameworks.

Combining TAM and Institutional Theory provides a comprehensive framework that considers both the individual-level factors influencing technology adoption and the broader institutional

contexts that shape and constrain these behaviors. This integrated approach can effectively address the complexities of implementing e-Governance policies in a way that enhances security in Nigeria.

Empirical Studies

This section provides a review of empirical studies on e-Governance policy and security around the globe. Kossakowski and Szuba (2024) employed a flexible incident response framework tailored to various organizational needs through case studies. Results showed that effective incident response plans significantly reduce recovery time and mitigate damage from cyber incidents, enhancing overall organizational security. Smith and Anderson (2024) carried out a Qualitative study of organizations' responses to cybersecurity incidents. Findings indicates that Organizations that systematically analyze and learn from cybersecurity incidents are more resilient and better prepared for future threats.

Institute for Security and Technology. (2024) Reviewed international cyber incident reporting frameworks and their effectiveness. The study found out that standardized global framework for incident reporting enhances international cooperation and cybersecurity resilience. Von Solms and Niekerk (2024) adopted a Systematic review of cybersecurity breaches and risk management strategies. Results revealed that Organizations that actively engage in incident reporting and analysis are better equipped to manage and mitigate cybersecurity risks. Vrbnjak et al. (2024) undertook an analysis of CIRS implementation across various healthcare settings. Findings shows that CIRS improves risk management by identifying and addressing systemic issues that compromise patient safety. Evans et al. (2024) carried out an Empirical study analyzing data from multiple healthcare facilities using electronic incident reporting systems (EIRS). Outcomes revealed that effective implementation of EIRS in healthcare leads to improved patient safety and organizational learning. Alshaikh et al. (2024) in their Systematic review of literature on cybersecurity incidents and organizational learning, discovered that organizations that systematically learn from incidents improve their cybersecurity resilience, developing better preventive measures.

Jahankhani (2024) carried out a comprehensive review of current trends and future directions in digital forensics. He found out that integration of AI, machine learning, and cloud computing are identified as key trends that will shape the future of digital forensics, enhancing the ability to handle complex investigations. Angelopoulou et al. (2024) conducted an Empirical analysis of forensic tools used in mobile device investigations. The study finds that mobile forensic tools are critical for extracting evidence from smartphones and tablets, with tools like Cellebrite and XRY providing robust capabilities for data retrieval and analysis. Nodeland and Jones (2024) in their Review of forensic techniques applied to social media platforms, found out that, Social media forensics can extract valuable evidence such as chat logs, images, and metadata. The study highlights the importance of these techniques in modern forensic investigations. Vondracek and Smith (2024) conducted a review of recent advancements in digital forensic tools and their application. Findings shows that advances in digital forensic tools have significantly enhanced the ability to detect, analyze, and prevent cybercrimes. Tools like Forensic Toolkit (FTK) and EnCase are highlighted for their comprehensive capabilities in handling complex forensic tasks.

Jahankhani (2024) conducted a Comprehensive review of current trends and future directions in digital forensics. The study revealed that integration of AI, machine learning, and cloud computing

are identified as key trends that will shape the future of digital forensics, enhancing the ability to handle complex investigations. Angelopoulou et al. (2024) carried out an Empirical analysis of forensic tools used in mobile device investigations. The study finds that mobile forensic tools are critical for extracting evidence from smartphones and tablets, with tools like Cellebrite and XRY providing robust capabilities for data retrieval and analysis.

Nodeland and Jones (2024) conducted a Review of forensic techniques applied to social media platforms. Results revealed that social media forensics can extract valuable evidence such as chat logs, images, and metadata. The study highlights the importance of these techniques in modern forensic investigations. Taylor (2021) adopted qualitative technique on focus groups to gather high school students' views on CCTV in schools. The study found out that Students felt CCTV increased their sense of security but also raised concerns about privacy and trust.

Jones and Smith (2021) explored the integration of AI in surveillance systems, assessing both the benefits and ethical implications. Findings revealed that AI-enhanced CCTV can improve crime detection and response times but raises significant privacy concerns. Lesniewski and Walczak (2020), conducted a study on CCTV surveillance systems in Poznan, Poland using qualitative method. Findings revealed that CCTV systems are cost-effective in reducing certain types of crimes, providing significant return on investment in terms of public safety. Kogut (2020) investigated effect of CCTV using Statistical analysis of the Katowice Smart Surveillance and Analysis System's impact on crime in public spaces over two time periods. Findings revealed that CCTV system significantly reduces crime rates, particularly for serious offenses, and enhances public safety.

Buys and Botha (2020) used Survey data collected from residents and security professionals to evaluate the perceived effectiveness of CCTV. Findings revealed CCTV was perceived as an effective deterrent, particularly when used in conjunction with other security measures. Welsh and Farrington (2020) conducted a systematic review and analyzed the impact of CCTV on crime rates and public perception in various countries. Findings revealed that there was a significant reduction in property and vehicle crime were noted, though the impact on violent crime was less clear. Piza et al. (2020) used meta-analysis to review 161 studies conducted between 1978 and 2017, evaluating the impact of CCTV on crime across different settings. CCTV was found to have a modest but significant effect on reducing crime, particularly in car parks and residential areas. Gill and Spriggs (2020) employed a quasi-experimental design to compare burglary rates in residential areas with and without CCTV. Results revealed the presence of CCTV was associated with a significant reduction in burglary rates, particularly when combined with other security measures.
From the extensive review of studies, the vast majority reveal that the Digital Incidence Reporting System significantly impacts security (Jones & Smith, 2021; Alshaikh et al., 2024; Smith & Anderson, 2024; Vrbnjak et al., 2024; Kossakowski & Szuba, 2024). However, all these studies primarily adopted qualitative techniques, which is a limitation as it results in a lack of empirical evidence to support their findings. Additionally, most studies on Digital Forensic Tools also used qualitative methods (Buys & Botha, 2020; Lesniewski & Walczak, 2020; Jahankhani, 2024; Vondracek & Smith, 2024). Similarly, research on CCTV Surveillance Systems (Gill & Spriggs, 2020; Piza et al., 2020; Welsh & Farrington, 2020; Buys & Botha, 2020; Taylor, 2021) predominantly utilized qualitative approaches. This creates an empirical gap that this study seeks to address. Therefore, this study aims to empirically analyze how e-Governance policies—

specifically Digital Incidence Reporting Systems, Digital Forensic Tools, and CCTV Surveillance Systems—affect security in Nigeria.

METHODOLOGY

This study adopts the cross-sectional descriptive survey design because date collection was done at a single point in time. Swain (2008) states that; descriptive survey design is used to gather data about the universe when the goal is to provide a systematic, factual, and accurate description as much as feasible. Furthermore, the researcher feels that this kind of design is appropriate since it eliminates the possibility of manipulating and controlling the population sample. Based on information from the Force Intelligence Department FID of Police Intelligence Department (FID) which comprises Intelligence Response Team (IRT) and Special Tactical Squad (STS), the study's population consists of the 806 police personnel at the force headquarters in FCT, Abuja. The researcher's choice for using the IRT and STS is because the units are saddled with the responsibility of tackling security issues in Nigeria. As such, information from these units is very reliable. The Yamane (1976) formula for sample size determination was adopted to establish the sample size. The formula is given as follows:

$$n = \frac{N}{1 + N(e^2)} \quad \ldots\ldots (1)$$

Where:

n=Minimum Sample Size

N= Population

1 =constant

E=margin of error (0.05)

Thus, substituting the population and the margin of error into the formula gives:-

$$\frac{N}{1 + N(e^2)}$$

$$= \frac{806}{1+806(0.05^2)}$$

$$= 267$$

Thus, the Yamane's calculation above suggests that the study's minimum sample size be 267. Both convenience and purposive sampling strategies was applied in the process of choosing study participants. Convenience sampling technique was used because of it is easy and quick to gather data from police personnel who are readily available, hence, only personnel of FID and IRT units within the force headquarters premises and inside their offices were utilized for the study. Because a conscious effort is made to guarantee that only personnel of the selected units were provided with the data collecting tools, the purposive sampling technique was used. Owing to the challenge of assessing the sample frame, the simple random sampling technique could not be used because it is nearly impossible to have all 806 police personnel available in one place for the purpose of sampling. Because of this, even with their drawbacks, our decision to use non-probability sampling approaches is justified.

Data collection was done using primary source of data collection. According to Olukotun et al. (2023), primary source of data collection is popular, effective and efficient in allowing respondents to provide answers to questionnaire instruments at their convenience. There are five sections in the questionnaire (A, B, C, D, and E). The purpose of the first portion is to get demographic data from the respondents and the information on each of the four study variables

were gathered in the subsequent sections, i.e., three independent variables and one dependent variable. Multiple choice questions were used to elicit information on respondents' demographic features such as gender, age group, highest educational qualification and the number of years in the service of the institution. In addition, a 5-point Likert scale having the ratings of "Strongly agree" (5) and "Strongly disagree" (1) was used to ask respondents to evaluate a set of attitudinal statements regarding variables under study. The justification for choosing a 5 likert scale is due to its precision, ease of understanding by respondent and flexibility of computation.

To address the cases of non-return and invalid cases, 30 percent was added to the minimum sample size making it a total of 354 structured questionnaires for distribution, as opposed to the 267 suggested by the sample size determination formula. This was suggested by Israel (1992) and was also adopted by many authors including Olukotun et al. (2023) and Yusuf et al. (2023). To analyze the data that was gathered for this study, both descriptive and inferential statistics was used. Descriptive statistics in the form of frequency table and percentages was used in data presentation, while inferential statistics in the form of multiple regressions was used to investigate the effect of e-Governance policy on security in Nigeria.
The dependent variable (Security) was regressed on the independent variables: Digital Incidence Reporting System (DIRS), Digital Forensic Tools (DFT) and CCTV Surveillance System (CCTV) using multiple regression model specified as follows:

$$EGB=b_0+b_1DIRS+b_2DFT+b_3CCTV+\varepsilon \quad \ldots\ldots\ldots (2)$$

Where:S= Security
b_0 = intercept,
b_1, b_2, b_3=Parameters or coefficient of the regression model,
DIRS= Digital Incidence Reporting Systems,
DFT= Digital Forensic Tools,
CCTV = CCTV Surveillance System
e=error term.
In measuring the variables, the study adopted indigenous measure development by developing the measure of the proxies for the independent and dependent variables from the scratch. This is so because of the researchers' intent to develop a measure that is tailored to the specific context being studied. Authors like Pollard-Terry et al. (2022), Lautenschlager et al. (2023) and Page et al. (2023) have used the same approach in their study.

To ensure that the questionnaire items are valid, a pilot test was conducted on 35 police personnel of the force head quarter. This is in line with the 10 per cent of the sample size recommended by Connelly (2008). Furthermore, the content validity was checked by two senior academics for necessary corrections. Olukotun et al. (2023) also adopted a pilot study to validate their questionnaire items. In addition, a reliability test was conducted through the adoption of Cronbach alpha coefficients. Cronbach alpha has been widely adopted by many authors, including but not limited to Olukotun et al (2023). This study also used the widely accepted criteria of a Cronbach alpha of 0.70 as the minimum acceptable level for attaining internal consistency (Gliem & Gliem, 2003).

RESULTS AND DISCUSSION

A total of 300 structured questionnaires were returned out of the 354 that were distributed; 300 of those, or 85 percent of the response rate, were determined to be credible. The minimum sample size of 267 suggested by the Yamane formula for determining sample size is exceeded by this 85 percent. The 300 valid answers are therefore appropriate for analysis and discussion.

Descriptive Analysis

The descriptive analysis of the respondents' demographic data is covered in this section. The results are shown in Table 5.

Table 5: Descriptive Results

Gender of the Respondents		
	Frequency	**Percentage**
Male	257	85
Female	43	15
Total	**300**	**100**
Age Group of the Respondents		
	Frequency	**Percentage**
18-25	24	8
26-35	53	18
36-45	147	49
Above 45	76	25
Total	**300**	**100**
	Highest	
Ph.D.	**Qualification**	1
Masters	3	11
First Degree/ HND	34	55
Diploma/NCE	165	29
Others	87	4
	11	
Total		**100**
	300	
Number of years in the UNIT		
	Frequency	**Percentage**
Less than 10	81	27
10-20	116	39
Above 20	103	34
Total	**300**	**100**

Source: Field Survey, (2024)

Most of the respondents, totaling 257 or 85% of the total, are men, according to Table 5's descriptive statistics. This is understandable considering the cultural and religious views of the research region, where men are more inclined than women. Most respondents are between the ages of 36 and 45, according to the descriptive data for the age distribution. Most responses appear to be mature, and it is expected that maturity would transcend or show in the caliber of

response. It's commonly believed that those who are more mature have a stronger sense of responsibility.

Additionally, table 5's display of the respondents' educational backgrounds shows that 3 or 1% of them hold a Ph.D., 34 or 11% have a master's degree, and 165 or 55% have a first degree or Higher National Diploma (HND). There are 87, or 29%, of the total responders who have at least an ND or NCE. This indicates that the bulk of responders have a high level of education, and their responses will be of the highest caliber.

Regarding years of service, Table 5's descriptive statistics indicate that 103 respondents, or 34%, have worked in the force headquarters for more than 20 years. This has also improved the quality of responses as majority of the respondents have adequate information on environmental knowledge management in the school.

Diagnostic Tests

Olukotun et al. (2023) state that diagnostic tests are carried out to make sure the outcomes are impartial and to stop the regression model's fundamental assumptions from being breached. In this regard, the diagnostic tests offered and covered in this subsection include the reliability, normality, auto-correlation, heteroskedasticity, and Collinearity tests. To verify the internal consistency of the study scales, a reliability test using Cronbach's alpha was carried out. The reliability test's Cronbach alpha findings are shown in Table 1.

Table: 1 Reliability Test using Cronbach Alpha

Variable	Cronbach's Alpha	Number of Items
DIRS	0.806	5
DFT	0.812	5
CCTV	0.789	5
Security	0.804	5

Source: Authors' Computation (2024)

According to Gliem and Gliem (2003), all of the variables in Table 1's reliability test findings have Cronbach's alpha coefficients over the minimally acceptable level of 0.70. It may be concluded from the reliability test findings that the questionnaire instruments are suitable for use as an internal consistency measurement.

More so, the study conducted normality using Skewness and Kurtosis to make sure that the regression model's normality assumption is not breached. The normality test results are displayed in table 2 below.

Table 2: Normality Test

	N	Skewness		Kurtosis	
	Statistic	Statistic	Std. Error	Statistic	Std. Error
DIRS	300	1.087	0.127	1.614	0.235
DFT	300	1.461	0.127	1.961	0.235
CCTV	300	1.554	0.127	1.767	0.235
Security	300	1.443	0.127	1.312	0.235

Source: Authors' Computation (2024)

None of the skewness or kurtosis numbers in table 2 are greater than two or seven, respectively. According to West et al. (1995), if these requirements are met, the variables in

the regression model are assumed to be normal and there is no violation of the normality assumption.

Furthermore, the Durbin-Watson (D-W) statistic was used to measure the results of the auto correlation test. According to Field (2009), there is no serial autocorrelation issue in this study, as indicated by the D-W statistics of 1.712, which is rather near to 2. Heteroskedasticity contradicts one of the fundamental assumptions of a regression model, which is the existence of constant variance of the error term. The study used a scatter plot graph approach to test for heteroskedasticity. The scatter plot graph displays the correlation between the residual (SRESID) and the predictive values of the independent variables (ZPRED). The scatter plot showed that the spots did not follow any particular pattern, which may indicate that the regression model does not contain heteroskedasticity.

In addition to heteroskedaticity, the study conducted a collinearity test which is primarily used to make sure two free variables, or independent variables in a model, do not have a correlation coefficient that is too high to be problematic (Achuku &Abubakar, 2023). A model's multicollinearity has the potential to skew the regression findings. Regression assumption is violated when there is multicollinearity, which is defined as high correlation among the explanatory variables in a model. Two widely used techniques for identifying multicollinearity—the variance inflation factor and the correlation matrix—were applied in the current study. The correlation values between the explanatory factors are shown in Table 3.

Table 3: Correlation

		DIRS	DFT	CCTV
DIRS	Pearson Correlation	1	0.614**	0.513**
	Sig.(2-tailed)		0.000	0.000
	N	300	300	300
DFT	Pearson Correlation	0.614**	1	0.537**
	Sig.(2-tailed)	0.000		0.000
	N	300	300	300
CCTV	Pearson Correlation	0.513**	0.537**	1
	Sig.(2-tailed)	0.000	0.000	
	N	300	300	300

**Correlation is significant at the 0.01 level (2-tailed).

Source: Authors' Computation (2024)

Note: DIRS= Digital Incidence Response Systems, DFT= Digital Forensic Tools and CCTV= CCTV Surveillance Systems.

The strongest correlation, which is 0.614 at the one percent significance level, is found between the DIRS and DFT, according to the correlation values in Table 3. According to Wooldridge (2015), multicollinearity is absent from the model since no two independent variables have correlation coefficients greater than .70. To validate the correlation's findings,

VIF was calculated and displayed in Table 4.

Table 4: Collinearity Statistics

Variable	Tolerance	Variance Inflation Factor
DIRS	0.548	1.823
DFT	0.515	1.924
CCTV	0.615	1.625

Source: Authors' Computation (2024)

Table 4 above shows that each independent variable's tolerance statistics is higher than 0.1 and that the corresponding VIFs are much lower than 10. Pallant (2005) confirmed that these two requirements indicate the lack of multicollinearity. This suggests that the VIF results have validated and supported the correlation's position about the lack of multicollinearity.

Regression Analysis

As stated in the methodology, regression technique is used in investigating the effect of e-Governance policy on security in Nigeria. The regression results of the study are shown in Table 6, which also includes t- and p-values and the coefficients of the variables and constant.

Variables/constant	Coefficients	t-values	p-values
Constant	10.321	10.543	0.000
DIRS	1.735	15.765	0.000
DFT	1.147	12.786	0.000
CCTV	2.164	26.117	0.000
R-square	0.724		
Adjusted R-square	0.745		
f-stats	332.071		
f-sig.			0.000
D-W	1.712		

Table 6: Summary of Regression Result
Source: Authors' Computation (2024)

The regression results in table 4.6 reveal that Digital Incidence Reporting Systems (DIRS) has a significant positive effect on security as confirmed by the t-value of 15.765, which is significant at 1 percent level of significance. Similarly, the regression results also show that Digital Forensic Tools (DFT) has significant positive effect on security as indicated by the t-value of 12.786, which is also significant at 1 percent level of significance. Furthermore, the regression results in table 6 indicate that CCTV Surveillance Systems (CCTV) has positive and significant effect on security as indicated by the high t-value of 26.117, which is also

significant at 1 per cent level.

Discussion of Findings

Based on the results of the regression analysis and the hypothesis testing, the conclusions are discussed. The null hypothesis one was rejected because digital incidence reporting systems was found to be positively and significantly associated with security at 1 percent level of significance. This suggests that the study is 99 per cent confidence in its decision to reject the null hypothesis one. The coefficient of digital incidence reporting systems which is 1.735 implies that a 1 percent increase in the use of digital incidence reporting systems is associated with about 1.73 percent increase in the level of security. This implies that if digital incidence reporting systems are available, such as being readily available online or within proximity, it can increase the likelihood of individuals seeking out and using this information. This result is in line with the findings of (Jones and Smith, 2021; Alshaikh et al. 2024; Smith and Anderson, 2024; Vrbnjak et al. 2024 and Kossakowski and Szuba,2024).

The null hypothesis two that states that use of digital forensic tools has a significant relationship with security was also rejected due to its significant t-value of 12.786. The coefficient of digital forensic tools 1.147 indicates that a 1 per cent increase in the digital forensic tools leads to about 1.14 percent increase in the level of security. By implication, if the digital forensic tools are used, there is a likely hood that tracking and detecting criminal activities can increase. This finding is also in concurrence with the findings of (Buys and Botha, 2020; Lesniewski and Walczak, 2020; Jahankhani, 2024 and Vondracek and Smith, 2024).

Lastly, null hypothesis three was also rejected because installation of CCTV surveillance systems was found to be positively and significantly associated with security at 1 percent level of significance. This suggests that the study is 99 per cent confidence in its decision to reject the null hypothesis three with a significant positive t-value of 26.117. Additionally, the coefficient of CCTV surveillance systems 2.164 indicates that a 1 per cent increase in installation of CCTV surveillance systems leads to about 2.16 percent increase in the level of security. CCTV surveillance systems have the highest coefficient and positive significant t-value among the variables under review. The highest coefficient suggests that CCTV surveillance systems have the greatest effect on security. The implication is that the use of CCTV has drastically reduced crime rate and improved security level in Nigeria. This result is also in agreement with the findings of (Gill and Spriggs, 2020; Piza et al. 2020; Welsh and Farrington, 2020; Buys and Botha 2020 and Taylor 2021

Additionally, the adjusted R-square of 0.745 indicates that digital incidence reporting systems, digital forensic tools and CCTV surveillance systems jointly account for 74% of the variation in security, with other factors or variables not covered or captured by the study accounting for the remaining 26%. The joint significance of the independent variables on the dependent variable is confirmed by the f-statistic of 332.071, which is significant at the 1 percent level. This suggests that the model is fit, and the findings, discussion, conclusion, and recommendations are valid.

CONCLUSION AND RECOMMENDATIONS

This study investigated the effect of e-Governance policy on security in Nigeria using the force headquarters in FCT Abuja. Three proxies of e-Governance policy such digital incidence reporting systems, digital forensic tools and CCTV surveillance systems were used as independent variables. On the other hand, the dependent variable used for this study is security and was measured using five items scale with a Cronbach's alpha coefficient of 0.804 which was adjudged as very reliable. The major findings reveal that digital incidence reporting systems has significant positive relationship with employees' green behavior; digital forensic tools have significant positive effect on security; and CCTV surveillance systems has significant positive effect with security in Nigeria.

Recommendation

The primary findings and conclusion lead to the following recommendations for policy implications:

i. Nigerian government should Partner with international organizations and experts to provide specialized training and certification programs for Nigerian security personnel.
ii. Establish continuous monitoring and evaluation mechanisms to assess the performance and impact of digital incidence reporting systems, digital forensic tools, and CCTV surveillance.
iii. Implement strict data privacy and security measures to protect sensitive information collected through digital incidence reporting systems and CCTV surveillance.
iv. Conduct public awareness campaigns to educate citizens about the importance and benefits of digital incidence reporting systems and CCTV surveillance.
v. Collaborate with private sector entities to leverage their expertise, technology, and resources in enhancing digital security measures.
vi. Allocate sufficient resources for the procurement, maintenance, and upgrade of digital incidence reporting systems, digital forensic tools, and CCTV infrastructure.
vii. Develop and enforce robust legal and regulatory frameworks that mandate the use of digital tools for crime reporting, investigation, and surveillance.
viii. Implement comprehensive training programs for law enforcement personnel and relevant stakeholders on the use of digital incidence reporting systems, digital forensic tools, and CCTV surveillance systems.

Limitation

One limitation of this study is that it was conducted on a single security outfit police in Nigeria, so the results may not be generalizable to other security outfits like military, department of state security DSS, Nigeria Civil Defense Corps, NIA, etc. Additionally, the study relied on self-reported data from the personnel, which may be subject to bias. More so, the study used convenience sampling technique. To overcome these limitations, future studies could use a more diverse sample and use objective measures of security. Additionally, future studies could use random sampling technique and, focus on other aspects of e-Governance, such as evaluating national crime database, mobile policing Apps, Community policing reforms and training of security personnel.

References

Achuku, A., &Abubakar, A. (2023). Effect of advertising on the consumer buying behavior of new products in Ajinomoto Foods Nigeria Limited, Katsina-Nigeria. *Journal of Business & Management, 1*(4), 274-296.

African Union. (2015). Agenda 2063: The Africa we want. African Union Commission. https://au.int/en/agenda2063/overview

Aguolu, C. C., &Aguolu, I. E. (2002). Libraries and information management in Nigeria: Seminal essays on themes and problems. *Ed-Linform Services*.

Alshaikh, M., Maynard, S. B., Ahmad, A., & Chang, S. (2024). Learning from cyber security incidents: A systematic review. *Journal of Information Security and Applications*, 10(1), 14-28. https://www.sciencedirect.com/science/article/pii/S1363412718300327

Angelopoulou, O., Jones, A., Horsman, G., & Pourmoafi, S. (2024). Cyber forensic analysis of mobile devices: Methodologies and tools. *Journal of Digital Forensics, Security and Law*, 18(2), 111-126. https://commons.erau.edu/jdfsl/vol18/iss2/5

Baldwin, D. A. (1997). The concept of security. *Review of International Studies*, *23*(1), 5-26. https://doi.org/10.1017/S0260210500118373

Buys, A., & Botha, S. (2020). Perceptions of the effectiveness of security measures used at security estates. *Security Journal, 33*(3), 455-474. https://doi.org/10.1057/sj.2020.18

Buzan, B. (1991). People, States & Fear: An Agenda for International Security Studies in the Post-Cold War Era. Harvester Wheatsheaf.

Carrier, B. (2005). File system forensic analysis.

Chen, Y., Iyer, R. S. H., & Smith, H. J. (2010). E-government strategies for disaster preparedness and response. Journal of Information Privacy and Security.

Chuku, C., Abang, D., & Isip, I.-A. (2019). Growth and fiscal consequences of terrorism in Nigeria. *Defence and Peace Economics, 30*(5), 549–569. https://doi.org/10.1080/10242694.2017.1389583

Connelly, L. M. (2008). Pilot studies. *Medsurg Nursing, 17*(6), 411-2.

Corcoran, P.B., Walker, K.E., Wals, E. J. (2004). Case studies, make-your-case studies, and case stories: A critique of case-study methodology in sustainability in higher education. *Environ. Educ. Res.* 10, 7–12.

Cordero, E.C., Todd, A.M., Abellera, D. (2008). Climate change education and the ecological Footprint. *Bull. Am. Meteorol. Soc.* 89, 865–872.

DiMaggio, P. J., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review, 48*(2), 147-160. https://doi.org/10.2307/2095101

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly*, *13*(3), 319-340. https://doi.org/10.2307/249008

Evans, S. M., Berry, J. G., & Smith, B. J. (2024). The use of electronic incident reporting systems: Influencing factors. *International Journal for Quality in Health Care*, 15(3), 141-150. https://www.sciencedirect.com/science/article/pii/S0168851018301264

Field, A. (2009). *Discovering statistics using SPSS* (3rd ed.).Sage Publishers Ltd.

Garfinkel, S. L. (2010). Digital forensics for network, internet, and cloud computing.

Gill, M., &Spriggs, A. (2020). How effective are residential CCTV systems: Evaluating the impact on burglary rates. *Security Journal, 33*(4), 563-579. https://doi.org/10.1057/sj.2020.12

Gill, M., &Spriggs, A. (2005). *Assessing the impact of CCTV*. Home Office Research, Development and Statistics Directorate.

Gliem, J. A., &Gliem, R. R. (2003). Calculating, interpreting, and reporting Cronbach's alpha reliability coefficient for Likert-type scales. Retrieved from https://scholarworks.iupui.edu/handle/1805/344

Hughes, L. J., Owen, A., &Terras, M. (2014). Utilization: A framework for understanding digital resource reuse. *Journal of Documentation*, *70*(2), 306-325.

IFAC. (2024). E-Governance as an anti-corruption strategy: The Nigerian experience. International Federation of Accountants. Retrieved from https://www.ifac.org/knowledge-gateway/contributing-global-economy/discussion/e-governance-anti-corruption-strategy-nigerian-experience

Jahankhani, H. (2024). Digital forensics: Trends and future directions. *International Journal of Electronic Security and Digital Forensics*, 15(1), 98-113. https://www.inderscience.com/jhome.php?jcode=ijesdf

Jones, K., & Smith, A. (2021). AI-powered public surveillance systems: Why we might need them and ethical concerns. *Science and Engineering Ethics, 27*(3), 1-15. https://doi.org/10.1007/s11948-021-00277-4

Kassel, K., Rimanoczy, I., Mitchell, S.F. (2016). The sustainable mindset: Connecting being, thinking, and doing in management education. *Acad. Manag. Annu. Meet. Proc.* (1) 16659.

Kogut, B. (2020). Urban video surveillance as a tool to improve security in public spaces. *Sustainability, 12*(15), 6210. https://doi.org/10.3390/su12156210

Kossakowski, K.-P., &Szuba, T. (2024). Cyber incident response and planning: A flexible approach. *Journal of Cyber Security and Information Systems*, 9(2), 121-135. https://www.sciencedirect.com/science/article/pii/S1877050919301434

Institute for Security and Technology. (2024). Cyber incident reporting framework: Global edition. *Journal of Cyber Policy*, 12(2), 100-115. https://securityandtechnology.org

Isola, L. A., Ayopo, B. A., Abiola, A., & Joseph, I. O. (2019). Examining the linkages between economic growth and terrorism: Evidence from Nigeria. In R. C. Das (Ed.), *The impact of global terrorism on economic and political development* (pp. 353–377). Bingley: Emerald Publishing Limited.

Israel, D. D. (1992). Sampling the evidence of extension program impact. Program evaluation and organizational development, IFAS, university of Florida, PEOD-5. www.edis.ifas.edu/pdffiles/p.

Jones, H. R., & Leonard, M. L. (2020). Improving incident reporting and response with digital solutions. *International Journal of Information Management*.

Kruse, W. G., &Heiser, J. G. (2002). *Computer forensics: Incident response essentials*.

Meier, A. (2015). *Digital governance and e-safety: Frameworks for public protection and emergency response*. Proceedings of the International Conference on E-Government.

Meyer, J. W., & Rowan, B. (1977). Institutionalized organizations: Formal structure as myth and ceremony. *American Journal of Sociology*, *83*(2), 340-363. https://doi.org/10.1086/226550

National Bureau of Statistics, Nigeria. (2020). Crime statistics: Reported offenses and the administration of justice. National Bureau of Statistics. https://nigerianstat.gov.ng/elibrary

Nodeland, B., & Jones, A. (2024). Social media forensics: Techniques and applications. *Journal of Digital Investigation*, 11(2), 78-92. https://www.sciencedirect.com/science/article/pii/S174228761830086X

Norris, C., & Armstrong, G. (1999). *The maximum surveillance society*: The rise of CCTV. Berg.

Nunamaker Jr., J. F., McGinnis, D. D., & Chen, H. (2009). E-government: A framework for e-safety in disasters and crisis management. Government Information Quarterly.

Olukotun, O., Gbolagade, O. L., &Abubakar, A. (2023). Cashless Policy and Patronage in Stanbic IBTC Bank Plc, Katsina-Nigeria, *Journal of Business & Management, 1*(3), 225-243.

Pallant, J. (2005). SPSS survival manual: *A step by step guide to data analysis using SPSS for windows (version 12).* Allen and Urwin. Barloz publishers INC.

Piza, E. L., Welsh, B. C., Farrington, D. P., & Thomas, A. L. (2020). The effect of CCTV on public safety: A meta-analysis. *Journal of Quantitative Criminology, 36*(2), 275-295. https://doi.org/10.1007/s10940-019-09432-2

Pollard-Terry, L., Nickerson, L., Leschied, A., Dush, J., Steinbach, R., &Breslin, F. (2022). An indigenous social work practice assessment: Development and validation of the social work practice assessment of processes and outcomes (SWPA) tool. *The British Journal of Social Work, 52*(2), 738-756. doi:10.1093/bjsw/bcac.

Smith, J. M., & Anderson, K. (2024). Learning from cybersecurity incidents: Organizational impact and mitigation strategies. *Journal of Cybersecurity and Privacy*, 7(1), 67-83. https://academic.oup.com/jcp/article/7/1/67/1923456

Swain, A.K.P.C. (2008).*A textbook of research methodology*. Kalyani Publishers.

Taylor, E. (2021). School surveillance in context: High school students' perspectives on CCTV. *Youth & Society, 53*(5), 755-774. https://doi.org/10.1177/0044118X20917060

United Nations Office on Drugs and Crime. (2019). Global study on homicide 2019. United Nations Office on Drugs and Crime. https://www.unodc.org/documents/data-and-analysis/gsh/Booklet1.pdf

Vondracek, T., & Smith, J. (2024). Digital forensic tools: Recent advances and enhancing the status quo. *Journal of Cyber Security and Information Systems*, 14(3), 215-229. https://www.sciencedirect.com/science/article/pii/S1877050919301434

VonSolms, R., & van Niekerk, J. (2024). Cyber risk and cybersecurity: A systematic review of data breaches. *Journal of Cybersecurity*, 8(1), 45-58. https://link.springer.com/article/10.1007/s10207-021-00507-9

Vrbnjak, D., Denktas, S., & Wu, A. W. (2024). Critical Incident Reporting System (CIRS): A fundamental component of risk management in healthcare. *Safety in Health*, 3(1), 32. https://safetyinhealth.biomedcentral.com/articles/10.1186/s40886-018-0072-5

Waltz, K. N. (1979). *Theory of International Politics*. McGraw-Hill.

Welsh, B. C., & Farrington, D. P. (2020). The internationalisation of CCTV surveillance: Effects on crime and public perception. *Criminology & Public Policy, 19*(4), 953-981. https://doi.org/10.1111/1745-9133.12456

Welsh, B. C., & Farrington, D. P. (2009). *Making public places safer: Surveillance and crime prevention*. Oxford University Press.

West, S. G., Finch, J. F., & Curran, P. J. (1995). Structural equation models with non normal variables*:* Problems and remedies. In R. H. Hoyle (ed.). Structural equation modelling: Concepts, issues and applications (pp. 56- 75). Thousand Oaks.

Wolfers, A. (1952). National Security as an Ambiguous Symbol. *Political Science Quarterly*, 67(4), 481-502. https://doi.org/10.2307/2145138

Wooldridge, J.M. (2015). *Introductory Econometrics: A Modern Approach*. Nelson Education.

Yamane, T. (1976). Statistics: *An introductory analysis* (2nd ed.). Harper & Row

Yusuf, A., Salaudeen, N. H., & Gbolagbade, L. O. (2023). An investigation of environmental knowledge management and employees' green behavior in a federal college of education. *Akungba Journal of Management, 5*(3), 124-138.

Yusuf, A., & Mohammad, S. (2023). Growth and fiscal effects of insecurity on the Nigerian economy. *The European Journal of Development Research, 35*, 743–769. https://doi.org/10.1057/s41287-022-00531-3