INTERNATIONAL JOUNAL OF: SCIENCE RESEARCH AND TECHNOLOGY

TIMBOU-AFRICA ACADEMIC PUBLICATIONS
INTERNATIONAL JOURNAL, FEBRUARY, 2022 EDITIONS
VOL. 8 NO. 9 ISSN: 2623-7861

IMPACT OF CYBER SECURITY ON POLICE INVESTIGATION OF CRIME IN KADUNA STATE

SULAIMAN USMAN DAN-GHANI; SAHALU BALARABE JUNAIDU; A. A. OBINIYI; & MUSTAPHA AMINU BAGIWA

Department of Computer Science, Ahmadu Bello University Zaria, Kaduna State, Nigeria.

ABSTRACT

Cybercrime has become widespread in a variety of industries, including banking, educational institutions, and social media networks, to name a few. Nigerian police have the constitutional authority to prosecute cybercrime, but the main problem is that

INTRODUCTION

Background of the study

The recent spate of widespread crimes in Nigeria has created a lot of uncertainty in the security situation, contributing to destabilization of citizens' social lives and property (Udoye, 2012). Internet fraud, ritual killings, armed robbery, drug trafficking, and abuse, as well as kidnapping, murder, and rape assassinations, are among the most difficult crimes that have been on the rise in recent years. Contract negotiations, embezzlement, and mismanagement are also on the rise in both the public and private sectors.

The assurance of protection is one of the most important tasks of every government's administration. The position is enshrined in the

there is no cyber security apparatus to assist in the investigation. The effect of cybersecurity on police investigations of crime in Kaduna state was investigated in this paper. Research questions and a descriptive survey were used in the study. This was based on primary data collected through a standardized questionnaire. The Taro Yamen formula was used in this analysis, and the population of the study included 197 and 132 sampled data. The findings revealed that there is a substantial correlation between cyber security and tracing of internet fraudsters in Kaduna state, as well as a notable correlation between cyber security and internet crime detection. According to the results of the investigation, Nigerian police should use the cybersecurity mechanism to significantly reduce crime.

Keywords: *Cybersecurity, Fraudster, Cybercrime, Warfare, Kaduna*

Federal Republic of Nigeria's 1999 charter, which states that "the security and wellbeing of the people will be the primary goal of the government" (Section 14(2)). (b). The government delegated domestic security to the Nigerian police force and civil defense in order to fulfill this responsibility. The Nigerian police force is tasked with detecting and stopping criminal activity, maintaining peace and order, and enforcing all laws and ordinances, all of which it is required to do flawlessly and correctly (Tope, 2009). Cyber security was introduced as a means of preventing internet fraud as a result of this.

Cybersecurity is concerned with preventing unauthorized access to and alteration of virtual systems and data hosted on the internet and through networks. The internet has evolved into a tool for conducting business, advancing and developing product in many bureaucracies, interacting with clients, and conducting financial activities (Wilson,

2015). The technology and strategies used to secure computers on networks and the internet, as well as information, from unwanted access, as well as vulnerabilities given by the Internet by cyber criminals, terrorist organizations, and hackers, are referred to as cybersecurity.

Information security and cybersecurity, according to Gai, and Qiu (2015), have been used interchangeably, with the latter perceiving the human's role in the security system as a new dimension, although the former did not, and the point of interest person still has a capacity target. However, such a conversation on cybersecurity has enormous ramifications because it focuses on the spiritual side of society as a whole. The term cybersecurity, on the other hand, has a wide range of implications, with features like secure sharing, confidentiality, and information access being used in crime prevention. However, the term cybersecurity has many diverse definitions, with diverse characteristics such as secure sharing, confidentiality, and access to information being employed in crime prevention. As a result, this research investigates the impact of cybersecurity on police investigations of crime in Kaduna State, and proposes the employment of cyber security technology in the security apparatus to aid in crime prevention and investigation.

The primary goal of this study is to look into the effect of cyber security on police crime investigations in Kaduna. The study aims to look at the effect of cyber security on internet crime in Kaduna state, as well as the impact of cyber security on tracing internet fraudsters in the state. The study adopts the research questions and a descriptive survey based on primary data collected through a standardized questionnaire. The Taro Yamen formula was used in analysing of the data, and the population of the study included 197 and 132 sampled data. The findings revealed that there is a substantial correlation

between cyber security and tracing of internet fraudsters in Kaduna state, as well as a notable correlation between cyber security and internet crime detection. According to the results of the investigation, Nigerian police should use the cybersecurity mechanism to significantly reduce crime.

The findings of this study will be of incredible benefits to financial institutions, the government, and potential researchers conducting state and national security evaluations. The findings will be extremely beneficial to financial institutions since they will measure the importance of cybersecurity in preventing financial loss. The findings will help the government ensure that financial institutions tackle the high percentage of digital crime in the economy. Furthermore, while the government is assuring full compliance with the cashless policy, cybercrime is increasing at an alarming rate.

Research Questions and Hypotheses

The following research questions guided the study

1. How does cybersecurity affect internet crime dictation in Kaduna state
2. How does cybersecurity affect the tracing of internet fraudster in Kaduna state

Hypotheses

The following null hypothesis guided the study

H_{01}: There is no significant correlation between cybersecurity and internet crime dictation in Kaduna state

H_{02}: There is no significant correlation between cybersecurity and tracing of internet fraudsters in Kaduna state

TIJSRAT
ISSN: 2623-7861

REVIEW OF RELATED LITERATURE

Overview of Cybersecurity

Cybersecurity is the process of protecting devices, networks, and application programs from digital threats. These attacks typically seek to acquire access to, manipulate, or destroy sensitive data; extort money from users; or impede standard business processes. Implementing successful cybersecurity standards is becoming increasingly difficult as there are more robots than humans and invaders become more innovative. The protection of computer networks, including hardware, software, and data, from cyber-attacks carried out over the internet is referred to as cybersecurity (Ngbokwe, 2012). Protection in the context of computing encompasses both cybersecurity and physical security, which are both used by businesses to prevent illegal access to data centers and other electronic networks. Information security is a subset of cybersecurity that focuses on ensuring the confidentiality, integrity, and availability of data (Tonge, & Kasture, 2013).

Elements of Cybersecurity

According to Biennier (2011), guaranteeing cybersecurity means coordinating efforts across all aspects of an information system, including application security, information security, network security, disaster recovery/business continuity planning, operational security, and end-user education.

Types of cybersecurity threats

It is a challenging task to stay up with new technology, security trends, and threat intelligence. It is, nonetheless, required in order to protect data and other assets from cyberthreats, which can take numerous forms.

TIJSRAT
ISSN: 2623-7861

- Ransomware is a sort of malware in which the attacker encrypts and locks the victim's computer system files, then demands payment to decrypt and unlock them.
- Malware, which includes worms, computer viruses, Trojan horses, and spyware, is any file or software that is designed to harm a computer user.
- Social engineering is a type of attack that uses human interaction to persuade users to violate security standards in order to obtain sensitive data that is normally protected.
- Phishing is a type of fraud in which fraudulent emails are sent that appear to be from legitimate sources but are intended to steal sensitive information such as credit card or login credentials.

Cybercrime

Defining the term "cybercrime" is crucial; yet, it is a challenging task that has far-reaching implications for not just legal concerns such as the scope of jurisdiction, but also practical studies aimed at assessing the effects of cybercrime on society as a whole. Because the accuracy of the information presented on the issue is so important in legislation, the definition of cybercrime serves as a foundation for quantitative measurement and qualitative classification. Despite numerous attempts to define ‘cybercrime' and categorize it, the following statement from a 1995 United Nations report attempting to define ‘computer crime' still remains true for the concept of cybercrime: “There is no guarantee even amongst the authors and experts who have attempted to arrive at meanings of computer crime that the phenomenon exists. The definitions that have been formed, on the other hand, are usually related to the subject for which they were written.

TIJSRAT
ISSN: 2623-7861

Cyber Security Techniques

a) **Access control and password security**

The concept of a user name and password has long been seen as a key method of protecting personal data. This could be one of the first cyber security measures taken.

b) **Authentication of data**

Before downloading, the documents we receive must always be authenticated, which means they must be reviewed to see whether they came from a trusted and credible source and if they have not been altered. Anti-virus software installed on the devices is frequently used to authenticate these documents. As a result, robust anti-virus software is also required to keep the devices safe from viruses.

c) **Malware scanners**

This is a program that searches all of the files and documents on the computer for malicious code or viruses. Viruses, worms, and Trojan horses are types of dangerous software that are frequently lumped together as malware.

d) **Firewalls**

A firewall is a piece of software or hardware that helps block hackers, viruses, and worms from accessing your computer via the Internet. All messages entering or leaving the internet pass through the firewall, which checks each communication and prevents those that do not match the security requirements. As a result, firewalls are critical in detecting malware.

e) **Anti-virus software**

Antivirus software is a type of computer application that identifies, stops, and eliminates dangerous software programs like viruses and worms. Most antivirus products have an auto-update capability that allows them to download new virus

TIJSRAT
ISSN: 2623-7861

profiles so that they can be checked for as soon as they are detected. Anti-virus software is a must-have for every computer system.

Theory of Model of IT Implementation Process (MIIP)

Kwon and Zmud (1978) presented the Model of IT Implementation Process (MIIP) hypothesis, which was further expanded by Cooper and Zmud (1990). Based on innovation, organizational change, and technology dissemination, the model presented a framework for guiding and organizing research. The initial model developed by Kwon and Zmud (1987) consisted of six stages: I initiation, (ii) organizational adoption, (iii) adaptation, (iv) acceptance and adoption, (v) routinization, and (vi) diffusion. MIIP appears to be a significantly more inclusive model than the majority of the models explored thus far. It considers intervening elements such as the technology being used, the organization, the environment, the task in focus, and the users' community characteristics, in addition to focusing on the six stages from adoption to dissemination of IT. MIIP looks to provide a strong theoretical foundation for ICT adoption and usage research. However, it's unclear whether MIIP can be used to give an adequate theoretical framework for a study on electronic fraud prevention and detection.

METHODOLOGY

Research Design

For this investigation, a descriptive survey design was used. People, attitude, belief, motivation, behavior, and views are the focus of descriptive survey research. According to Nworgu (2015), descriptive surveys are ideal for investigations that seek out people's opinions, attitudes, and perceptions in their natural environment.

Area of the Study

This study was carried out in Kaduna state Police command. The population of the study consist of 197 police men (intelligent squared).

Sampling Procedure

The data was analyzed using the Yaro Yamane formula for determining sample size. This is provided by:

$$n = \frac{N}{[1+N(e)^2\ ]}$$

Where: n= sample size.

N= population of interest, (which is 197)

e= error estimate/level of significance, which is normally 5%

Solving:

$$n = \frac{197}{[1+197(0.05)^2\ ]}$$

$$n = 132$$

Method of Data Analysis

With the help of Statistical Package for Social Science, the data will be analyzed using Pearson Product Moment Correlation (SPSS, Version 23)

The correlation formula is given below:

$$r^2 = \frac{n\sum xy - \sum x \sum y}{(n\sum x^2 - \sum(x)^2)(n\sum y^2 - \sum(y)^2)}$$

$$0 < r^2 < 1$$

DATAPRESENTATION AND ANALYSIS

TEST OF HYPOTHESES USING STATISTICAL PACKAGE FOR SOCIAL SCIENCE (SPSS, VERSION 23)

TIJSRAT
ISSN: 2623-7861

Decision rule: When the probability value is greater than the alpha value, we accept the null hypothesis; otherwise, we reject it.

Hypotheses I

H_0:There is no significant relationship between cyber security and internet crime dictation in Kaduna state

H_1:There is a significant relationship between cyber security and internet crime dictation in Kaduna state

Correlations

		Cyber security	Internet crime reduction
Cyber security	Pearson Correlation	1	.084
	Sig. (2-tailed)		.021
	N	5	5
Internet crime reduction	Pearson Correlation	0.84	1
	Sig. (2-tailed)	.021	
	N	5	5

Because the probability value (0.021) is less than the alpha value (0.05), the researcher accepts the alternative hypothesis and concludes that cyber security and online crime dictation in Kaduna state have a significant with a correlation value of 0.84.

Hypotheses II

H_0:There is no significant relationship between cyber security and tracing of internet fraudster in Kaduna state

H_1:There is a significant relationship between cyber security and tracing of internet fraudster in Kaduna state

Correlations

		Cyber security	Tracing of internet fraud
Cyber security	Pearson Correlation	1	.91
	Sig. (2-tailed)		.013
	N	5	5
Tracing of internet fraud	Pearson Correlation	0.91	1
	Sig. (2-tailed)	.013	
	N	5	5

Because the probability value (0.013) is less than the alpha value (0.05), the researcher accepts the alternative hypothesis and concludes that there is a substantial relationship between cyber security and online fraudster tracking in Kaduna state, with a correlation value of 0.91.

CONCLUSION AND RECOMMENDATION

The findings of this research shows that there is a substantial relationship between cyber security and internet crime dictation in Kaduna state, as well as a substantial relationship between cyber security and internet fraudster tracing in Kaduna state, after. The researcher advises that Nigerian police employ a cyber security strategy to reduce crime based on the findings.

REFERENCES

Balogun, E. (2009). The Political Construction of Collection Insecurity from Moral Panic to Blame Avoidance and Organised Irresponsibility. Centre for European Studies Working Paper series 126.

Biennier, A. (2011).Attack detection and identificationin cyber-physical systems. IEEE Transactions on AutomaticControl, 58(11):2715–2729, 2013.

Fried, G. (2015).Proactive attributebasedsecure data schema for mobile cloud in financial industry. InThe IEEE International Symposium on Big Data Security on Cloud,pages 1332–1337, New York, USA.

Gai, A. & Qiu, K. (2015).Securityawareoptimization for ubiquitous computing systems with SEAT graph approach, *Journal of Computer and System Science, 79(5):518–529, 2013.*

Gottschalk , C. (2007). Corruption in Nigeria; Terrorism in Nigeria. University of Ibadan Press, Ibadan

Igbokwe, B. (2012).Influence of cyber security on fraud control *Journal of Computer Science, 3(2):36–39.*

Ngbokwe, T.(2012). Vulnerability assessment ofcybersecurity for scada systems. IEEE Transactions on PowerSystems, 23(4):1836–1846, 2008.

Nigeria Police Force (2008). Annual Report of the Nigeria Police Force,. Ikeja 'F' Department of the Nigeria Police.

Nworgu, B.G. (2015). Educational research: Basic issues and methodology. Enugu: University Trust Publishers.

Nworgu, B.G. (2015). Educational research: Basic issues and methodology. Enugu: University Trust Publishers.

Odekunle, N (2014). Kidnapping, Security Challenges and Socio-economic Implications to the Niger Delta Region of Nigeria. Central Point Journal: *A Journal of Intellectual Scientific and Cultural Interest*. 16, (2). 205-216.

Tonge, Q.& Kasture, F. (2013).A survey on cyber securityfor smart grid communications. IEEE Communications Surveys &Tutorials, 14(4):998–1010, 2012.

Tope, B. (2009). The Nigeria Police Law with Police Act and Code of Conduct. Lagos, Ikeja, Princeton and Associates Publishing Company Limited. Pp 33.

Udoye, O. M (2013). Security Challenges in Nigeria and the Implications for Business Activities and Sustainable Development, *Journal of Economics and Sustainable Development* , l4, (2), 79-99

Ugwu, E.E.O. (2010). Police Community Relation in Nigeria; What Went Wrong? Paper Presentation at the Seminar on Role and Function of the Police in a Post Military Era, organized by the Centre for Law Enforcement Education in Nigeria (CLEEN) Lagos and the National Human Commission.

Ugwuoke, J (2011). Security Challenges in Nigeria and the Implications for Business Activities and Sustainable Development Journal of Economics and Sustainable Development. Vol. l4, (2), pp 79-99

Wilson, H. (2015).A survey on security issues inservice delivery models of cloud computing, *Journal of network and computer applications*, 34(1):1–11.