International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 5 Issue 6, September-October 2021 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Strategic Database Security Management and Cybercrime Reduction among Youths in Information Technology Companies in Nigeria

Agbeche, Aaron[1]; Elechi, Bobby Chime[2]; Okechukwu, Prince Jumbo[2]

[1]Michael and Cecilia Ibru University, Ughelli, Nigeria
[2]Rivers State University, Port Harcourt, Nigeria

ABSTRACT

The purpose of this study is to investigate the relationship between strategic database security management and cybercrime reduction among youth in Information Technology sector in Nigeria. Cross sectional survey design was used for this study. The population of the study comprises 32 information and technology companies in Rivers state. The method of data collection was questionnaire. Data from the distributed questionnaire was further analyzed, using the spearman rank order Correlation Coefficient. The hypotheses of the study were tested through the help of Statistical Package for Social Science (SPSS), version 20. Findings revealed that strategic database security management have a significant relationship between the measures cybercrime reduction among youth in information technology companies in Nigeria. Therefore, we recommend that Management of information technology companies should ensure that proper computer security measures are put in place in order to fortify their database from unauthorized persons.

KEYWORDS: *Database Security Management, Database resilience, Improved Database Security*

How to cite this paper: Agbeche, Aaron | Elechi, Bobby Chime | Okechukwu, Prince Jumbo "Strategic Database Security Management and Cybercrime Reduction among Youths in Information Technology Companies in Nigeria" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-5 | Issue-6, October 2021, pp.1592-1597, URL: www.ijtsrd.com/papers/ijtsrd47643.pdf

IJTSRD47643

1. INTRODUCTION

In this present global village, the desire to reduce the level of cyber fraud or crime among the ever growing population cannot be over emphases. Statistically, all over the world, there has been a form of cybercrime committed every day since 2006. It is this global fear of cybercrime that has led to the continuous clamoring to have in place institutions and regulatory bodies that will help stop or reduce the menace of cybercrime among the growing youthful population in Nigeria. To achieve this, so many scholars have tried to research into the cause of such crime and why the youth have taken to it has a way of life. As a result of this issue, scholars has propagated the issue of strategic database security management as a best way to help reduce such global epidemic that has made life miserable for some families, individuals and the organizations as a whole.

The construct strategic data base security management cannot be discuss without looking at data base management. A database management is a collection of interrelated data and a set of programs to access those data. These collected of data, usually referred to as the database contains information relevant to an individual or enterprises (Morrison, 2013).Originally, the primary goal of a database management is to provide a way to store and retrieve information in both convenient and efficient manner. For Steve and Smith (2015) database management is designed to manage large bodies of information; as the management of data involves both defining structures for storage of information and providing mechanisms for the manipulation of such information which has given room to the high level of crime found among the youthful population in Nigeria. In addition, the database system must ensure the safety of the information stored, despite system crashes or attempts at unauthorized access. If data are to be

shared among several users, the system must avoid possible anomalous results (Philips, 2014).

On the other hand, over the past twenty years, immoral cyberspace users have continued to use the internet to commit crimes; this has evoked mixed feelings of admiration and fear in the general populace along with a growing unease about the state of cyber and personal security. This phenomenon has seen sophisticated and extraordinary increase recently and has called for quick response in providing laws that would protect the cyber space and its users. According to the Indian Express (2002) an underworld don in a hospital was to undergo a minor surgery. His rival went ahead to hire a computer expert who altered his prescriptions through hacking the hospital's computer system. He was administered the altered prescription by an innocent nurse, this resulted in the death of the patient.

The incidents of cybercrime first raised it head in 2002 (Indian Express, 2002), Prior to the year 2002, the phenomenon of cybercrime was not globally associated with Nigeria. This resonates with the fact that in Nigeria came into realization of the full potential of the internet right about that same time. Since then, however, the country has acquired a worldwide notoriety in criminal activities, especially financial scams, facilitated through the use of the Internet. Nigerian cyber criminals are devising new ways of perpetrating this form of crime and that the existing strategies of tracking these criminals are no longer suitable to deal with their new tricks (Morrison, 2014).As measures and techniques for detecting crimes and criminals advances continue to come into existence, criminals also look for means of hiding from these measures and the Internet currently serves as a hiding place for fraudsters who have simply migrated from the streets to an electronic platform offered by the World Wide Web.

Different nations have adopted different strategies to contend with crimes depending on their nature and extent. Certainly, a nation with high incidence of crime cannot grow or develop. That is so because crime undermines development. It leaves negative social and economic consequence (Sylvester, 2012). For Nigeria, a nation in the process of saving her face regarding cybercrimes; efforts are now being directed at the sources and channels through which cybercrimes are perpetuated.Ejiekwu(2017) was of the view that majority of the cybercrimes perpetrated in Nigeria generally are targeted at individuals and not necessarily computer systems, hence they require less technical expertise and as a consequence, the damage done manifests itself in the real world. For Agatha (2016) in Brito, Fontes, Miquelina, & Guevara (2018) she did not only look at the extent of the crime but went on to write on the challenges in fighting cybercrimes today; by stressing the fact that cybercrimes have been in existence for only as long as the Global Information Infrastructure exists. This explains the unpreparedness of society and the world in general towards combating them. Cybercrime has caused lot of damages to individuals, organizations and even the Government.

The issue that this works intends to address is the malicious activities and attack on their computer systems which has led to lose of sensitive data, disruption of work, damage to the brand image, and company reputation and the individual bases, the loss of cash and lives of victims of this cybercrimes. It is in pursuit of an understanding of how to reduce cybercrime that the paper seeks to examine different strategic database security management that can help us reduce the cybercrime among Nigeria youth. It is therefore imperative to examine the impact of strategic database security management and cybercrime reduction in information technology in rivers state, Nigeria. The purpose of this study is to determine how database security management and cybercrime reduction among Nigeria youths. The study has as an objective to determine how strategic database security management influences cybercrime reduction among Nigeria youths. With hypotheses which include:

H_{01}: There is no significant relationship between strategic database security management and improvement in cybercrime reduction among youths in Information Technology companies in Nigeria.

H_{02}: There is no significant relationship between strategic database security management and efficiency in cybercrime reduction among youths in Information Technology companies in Nigeria.

1.1. Conceptual Framework

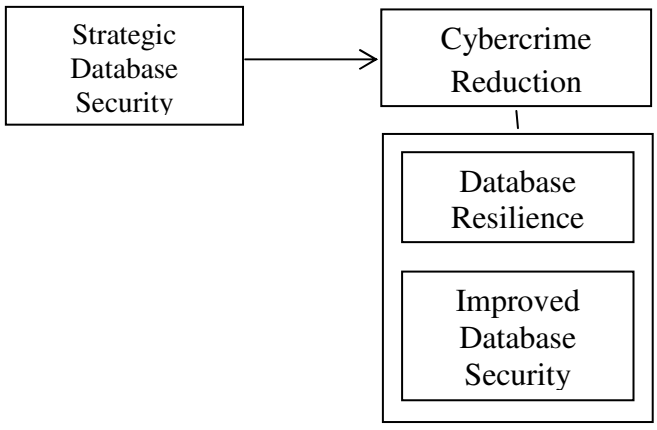

Figure 1.1: Conceptual framework
Fig 1.1. Source: Researcher's Conceptualization (2021)

2. Theoretical Foundation

A theoretical foundation or framework is lens from which all knowledge are constructed either metaphorically or literally for a research study. It serves as a structure and support or as the rational for the study. In search of theories of strategic database security management and cybercrime reduction a number of theories have been raised. This study looks at information processing theory. Information processing theory was originally propounded by George Miller. It is a cognitive theory that focuses on how information is encoded into our memory. The theory describes how our brains filter information, from what we're paying attention to in the present moment, to what gets stored in our short-term or working memory and ultimately into our long-term memory (Almutairi, 2017).

2.1. Strategic Database Security Management.

According to Heptinstall (2016), strategic database security management involves a variety of techniques, processes and practices for keeping business data safe and inaccessible by unauthorized parties. Strategic data security management systems focus on protecting sensitive data, like personal information or business-critical intellectual property. For example, data security management can involve creating information security policies, identifying security risks, and spotting and assessing security threats to IT systems. Another critical practice is sharing knowledge about data security best practices with employees across the organization (Jansen, 2015).

Some employees steal data or damage systems deliberately, for example, to use the information to set up a competing business, sell it on the black market or take revenge on the employer for a real or perceived problem. Users and admins can also make innocent but costly mistakes, such as copying files to their personal devices, accidently attaching a file with sensitive data to an email, or sending confidential information to the wrong recipient.Enhance, to build a layered defense strategy, it's critical to understand your cyber security risks and how you intend to reduce them. It's also important to have a way to measure the business impact of your efforts, so you can ensure you are making appropriate security investments.

For organization or individual to check the level of insecurity he or she is exposed to such entities must adhere to operational and technical best practices to mitigate data security risks; such practice involve the use of compliance requirements as cybersecurity basics. Compliance regulations are designed to force companies defends against major threats and protects sensitive data. Although meeting compliance requirements is not sufficient for complete data security, it will help you get started on the right path to risk management and data protection (Albaity, 2012). Also, having a clear cybersecurity policy helps to also check cybercrimes rate. Create a policy that clearly explains how sensitive data is to be handled and the consequences for violating your data protection. Making sure all employees read and understand the policy will reduce the risk that critical data will be damaged or lost due to human actions (Johnson, 2015).

Furthermore, build and test a backup and recovery plan. Companies must prepare for a range of breach scenarios, from minor data loss to complete data center destruction. Ensure that critical data is encrypted, backed up and stored offline. Set up roles and procedures that will speed recovery, and test every part of the plan on a regular schedule (Hoffman, 2016). Have a bring-your-own-device policy**.** Allowing users to access your network with their personal devices increases the risk of a cyber-security Therefore; create processes and rules that balance security concerns against convenience and productivity. For instance, you can mandate that users keep their software up to date. Keep in mind that personal devices are harder to track than corporate devices (Halters, 2011).

2.2. Cybercrime Reduction.

Cybercriminals are maliciously seeking to lockout critical systems preventing staff from accessing vital resources needed during pandemic until a ransom is paid. Cybercriminals are taking advantage of all businesses who are increasingly working under extreme pressure and more frequently are doing so remotely, which for many is a new concept and therefore they may not be as focused on cyber security as they usually would be. Cybercriminals continue to use phishing attacks to target businesses but the scams are now Covid-19 related by purporting to come from charities seeking donations or impersonating governmental bodies or contain information about treatments for the virus. Users are asked to click on attachments or links which in turn leads them to malicious websites allowing cybercriminal access to sensitive data and financial information.

Resilience

Most enterprise organizations can't operate without computers. Digitized data is an intrinsic part of the corporate knowledge base. If you lose the data, you might harm the business beyond recovery. Resiliency protects the corporate knowledge base and saves the corporation from lost time. When a failure occurs

with hosted data, data resiliency allows data to remain available to traditional applications and applications that incorporate APIs and other services for analytics. Choosing the correct set of data resiliency techniques and technologies in the context of an overall business continuity plan is vital, but it can be complex and difficult*(Jopkins,2017).*

Management Improvement

The rapid development and proliferation of information technology has offered many opportunities for integrated business operations. It has enabled business enhances their efficiency and effectiveness in operations such as customer care, sales, human resources and production. However, these developments have served to bring issues of security. Many firms are falling victims of cybercrimes. This is occasioned by unauthorized access, which makes data lose its integrity and lastly operations of the business are affected negatively (Singh, 2009).

3. Methods

The research dessign adopted in this study is the survey research design vis-à-vis correlational study. The target population of this study was seventeen (17) organization and fifteen (15) individuals that has been a victim of this cybercrime. Survey questionnaire was the major means of gathering primary data.The information collected from the questionnaire was summarized in their groups and inferential statistical tool of spear man rank order colorations was applied to test the level of significance among variables and finally, the analysis was aided with SPSS version 21.0.

3.1. Findings

Result and Frequency Analysis

Mean scores and standard deviations are illustrated. The presentation begins with the independent variable which is strategic data security management. It then proceeds to the dependent variable which is cybercrime reduction. These are all scaled on the five (5) point Likert scale (ranging from 1: **SD**=strongly disagree, 2: **D**=disagree, 3**: N**=neutral, 4: **A**=agree and 5: **SA**= strongly agree). The secondary data analysis was carried out using the Spearman rank order correlation tool at a 95% confidence interval. Specifically, the tests cover hypotheses HO_1 to HO_2 which were bivariate and all stated in the null for.

Table 1 showing descriptive statistics for Strategic Database security management

Statistic	N	Minimum	Maximum	Mean	Std. D
Strategic Database security management	174	1.00	4.00	3.4538	.76604
Valid N (list-wise)	174				

Source: Research Data 2021 (SPSS output version 20.0)

Table 1 illustrates the descriptive statistics for the independent variable. Strategic database security management carry high mean scores (x>2.0) based on the 5-point Likert Scaling adopted.

Table 2: Showing Descriptive Statistics for Measures of Cybercrime reduction

	N	Minimum	Maximum	Mean	Std. deviation
Resilience	174	1.00	4.00	3.6846	.76684
Management improvement	174	1.00	4.00	3.3692	.70135
Valid N (listwise)	174				

Source: Research Data 2021 (SPSS output version 20.0)

Table 2 illustrates the descriptive statistics for the measures of the dependent variable. All two measures carry high mean scores (x>2.5) based on the 5-point Likert Scaling adopted.

H_{01}: There is no significant relationship between strategic database security management and improvement in cybercrime reduction among youths in Nigeria.

H_{02}: There is no significant relationship between strategic database security management and management improvement in cybercrime reduction among youths in Nigeria.

Table 3: Correlation Matrix for database security management and cybercrime reduction

		Strategic Database security management	Organizational Resilience	Management improvement
Database security management	Pearson Correlation	1	.882**	.964**
	Sig. (2- tailed)		.000	.000
	N	174	174	174
	Pearson Correlation	.88**	1	.923**

Database resilience	Sig. (2- tailed) N Pearson Correlation	.000 174 .964**	 174 .923**	.000 174 1
Improved database security	Sig. (2- tailed) N	.000 174	.000 174	 174

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

The table 3 correlation of hypothesis one and two; the hypothesis one shows a significant correlation at r = .882** where P-value = .000 (P>0.001). This implies a strong and significant relationship between both variables at 95% level of confidence. We therefore reject the null hypothesis (Ho: 1), and restated, thus, there is a significance relationship between strategic database security management and resilience. The hypothesis two shows a significant correlation at r = .964** where P-value = .000 (P<0.001). This implies a strong and significant relationship between both variables at 95% level of confidence. We therefore reject the null hypothesis (Ho:2), and restated, thus, there is a significance relationship between database security management and management improvement.

Discussion of Findings

The first and second hypothesis shows that there is a strong positive relationship between database security management and each of the measures of cybercrime reduction in the among youths in Nigeria. This finding support the study conducted by Morgeson et al., (2013), when they stated that, since then, there has been a growing volume of research exploring how to bring these elements together so that jobs can be designed both to maximize the engagement and satisfaction of individual workers on the one hand, and maximize the productivity and performance of organizations on the other. There is now considerable evidence that individuals' experience of their day-to-day work directly affects their engagement levels, and also their personal effectiveness.

4. Conclusion

Proper database management helps increase organizational accessibility to data, which in turn helps the end users share the data quickly and effectively across the organization without giving room for cybercrime to perpetrate their act. A proper database management helps get quick solutions to database queries, thus making data access faster and more accurate. End-users like salespeople will have enhanced access to the data, enabling a faster sales cycle and a more sound decision making. Implementing a database management promotes an integrated picture of an organization's operations. It becomes easy to see how processes in one segment of the organization affect other segments. Most importantly, with the right tools and software applications put in place in pursuit of database management, it will be difficult for cyber criminals to penetrate the organization's database.

Recommendation

Accordingly, the study strategy and methodology were designed in a way that points towards the achievement of the study objectives. The study concludes that database management through the use of database security management significantly influences organizational resilience and management improvement. Based on the discussions and conclusions above, the following recommendations are hereby made:

1. Management of information technology companies should ensure that proper computer security measures are put in place in order to fortify their database from unauthorized persons.
2. Management of organizations should ensure all organization's data have a secure duplicate in case of data loss, as this will help them recover every data.
3. management of organizations should ensure that all sensitive data are encrypted in such that only authorized personnel can decrypt the code, as this will help mitigate the frequency of cyber-attacks on organization's database

Reference

[1] Morgeson, F. P., Aguinis, H., Waldman, D. A., & Siegel, D. S. (2013). Extending corporate social responsibility research to the human resource management and organizational behavior domains: A look to the future. *Personnel Psychology*, *66*(4), 805-824.

[2] Hopkins, W. G. (2017). Spreadsheets for analysis of validity and reliability. *Sport science*, *21*.

[3] de Willebois, E. V. D. D., Sharman, J. C., Harrison, R., Park, J. W., & Halter, E. (2011). *The puppet masters: How the corrupt use legal structures to hide stolen assets and what to do about it*. World Bank Publications.

[4] Johnson III, J. A., & Johnson, A. M. (2015). Urban-rural differences in childhood and adolescent obesity in the United States: a systematic review and meta-analysis. *Childhood obesity*, *11*(3), 233-241.

[5] Albaity, M., &Rahman, M. (2019). The intention to use Islamic banking: an exploratory study to measure Islamic financial literacy. *International Journal of Emerging Markets*.

[6] Wang, X. H., Fang, Y., Qureshi, I., & Janssen, O. (2015). Understanding employee innovative behavior: Integrating the social network and leader–member exchange perspectives. *Journal of organizational behavior*, *36*(3), 403-420.

[7] Bath, P. M., Woodhouse, L. J., Appleton, J. P., Beridze, M., Christensen, H., Dineen, R. A.,... & Broughton, D. (2018). Antiplatelet therapy with aspirin, clopidogrel, and dipyridamole versus clopidogrel alone or aspirin and dipyridamole in patients with acute cerebral ischaemia (TARDIS): a randomised, open-label, phase 3 superiority trial. *The Lancet*, *391*(10123), 850-859.

[8] Johnson, N. J., He, S., Diao, S., Chan, E. M., Dai, H., &Almutairi, A. (2017). Direct evidence for coupled surface and concentration quenching dynamics in lanthanide-doped nanocrystals. *Journal of the American Chemical Society*, *139*(8), 3275-3282.

[9] Brito, P., Fontes, J. P., Miquelina, N., & Guevara, M. A. (2018, November). Agatha: Face benchmarking dataset for exploring criminal surveillance methods on open source data. In *2018 International Conference on Graphics and Interaction (ICGI)* (pp. 1-8). IEEE.

[10] Morrison, P., Moye, D., & Williams, L. A. (2014). *Mapping the field of software security metrics*. North Carolina State University. Dept. of Computer Science.